Guidelines for Artificial Intelligence-driven Enterprise Compliance Management Systems

Ana-Maria Wall

A thesis submitted in partial fulfilment of the requirements of
Edinburgh Napier University, for the award of
Doctor of Business Administration

January 2021

Abstract

The use of Artificial Intelligence (AI) to design and drive a Compliance Management System (CMS) at an enterprise level is a strategic decision to be taken by large organizations. Given the complexity this decision entails, conceptual guidelines addressed to senior management and board of directors are required. The original contribution to knowledge and practice of this research lies in the understanding of how compliance management systems are set-up in organizations, by using the CMS framework derived from literature, later confirmed by empirical data. Furthermore, this research originally contributes to both knowledge and practice, through the depiction of the enablers and barriers of AI adoption in organizations, as well as the recommended conceptual guidelines for AI-driven CMSs. Using three case studies as a research method, this paper investigates the current set-up of CMSs, as well as the enablers and barriers of AI adoption and then discusses the driving themes of strategic importance to organizations when sourcing AI aimed at supporting the management of compliance. These themes are: CMS components structures responsibilities, enablers and barriers of AI, control and compliance of AI applications, compliance by design, data governance and data management, cyber security, information technology infrastructure, regulation and regulators, and collaboration with external parties. The thematic findings of this research are additionally discussed in the context of the three lines of defence of an enterprise (business units, support functions, audit functions), making this an organizational framework for the design of an AI-driven CMS. The research concludes with the recommendations that in order to adopt an AI-driven enterprise CMS, organizations should do the following: strategically decide the type of AI organization they want to be, involve stakeholders in the design phase of new policies and AI applications, invest in data governance and IT infrastructure, tap on best practices from cyber security, and collaborate with external parties and regulators.

Disclaimer

This research and the collected and analysed data have been conducted prior to the COVID-19 global crisis. Therefore, this study is non-inclusive of considerations of consequences of COVID-19 actions on the management of compliance within organisations.

Acknowledgements

I would like to thank my family (Volker, Claudia, Sandra, Mirela, Constantin, Alexandra, Dan, Marc, Heidi) for all the support, encouragement and patience they have shown towards me over the past three and a half years since I embarked on the doctoral research journey.

I would like to express my deep and sincere gratitude to my research supervisor, Prof. Dr Morrison Handley-Schachler from Edinburgh Napier University in Scotland, for providing invaluable guidance throughout this research, grounding me, giving me objective and factual feedback, and for always being responsive. The stability of the supervision interactions allowed me to focus on my research and this made a significant contribution to my ability to balance the research with work-related responsibilities.

At the same time, I would like to thank Prof. Dr Stefan Hunziker from Lucerne University of Applied Sciences and Arts in Switzerland, for acting as my co-supervisor. His expertise in my topic and methods of research offered me a third pair of eyes as feedback on my evolution and the path of my research.

I would also like to express my appreciation to the entire Edinburgh Napier University academics, professors and staff, for their teaching, organization and guidance. Special thanks go to Dr Gerri Matthews-Smith and Dr Janice McMillan for their great leadership and teaching, as well as their contagious enthusiasm for research.

During the proposal phase, I've had wonderful guidance on the application process and the acceptance interviews. Thank you to Prof. Dr Gordon Millar from Lucerne University of Applied Sciences and Arts in Switzerland for this.

Please note that an editor has not been used in the construction of this thesis.

Glossary

Artificial Intelligence is a field of study, represented by computer systems and which is based on cognitive science (the study of thought, learning, and mental organization, which draws on aspects of psychology, linguistics, philosophy, and computer modelling).

Augmented Intelligence is considered in this paper as computer tools/applications that are augmenting human intellectual capacity.

Compliance by Design is an approach to manage compliance requirements by embedding business rules within applications and processes during the design phase.

Compliance Management System represents the cumulative actions of managing compliance within a framework of procedures and routines that enable the adherence to internal and external regulations and standards that emerge from both internal and external sources. The ultimate aim of a Compliance Management System is solving the problem of addressing internal and external risks to the organisation and its stakeholders.

Control of Artificial Intelligence represents the exercise of, and the ability to be in control over the mechanisms used by those computer systems augmenting human intelligence.

Cyber security represents the security of information and of other communication and automatic control systems.

Data governance represents the exercise of authority and control over the management of data.

Data management is the management of data used by the computer systems of an organization, data both acquired internally, or provided by third parties.

Governance Risk and Compliance is a business function in an organization providing organizations with a uniform view of information so it can align risk management with objectives, reduce complexity, diminish inconsistencies, and harness technology for desired outcomes.

Large organization in the context of this research is represented by an organization with more than 250 employees (as defined by the statistical office of the European Union) (Eurostat, n.d.). Therefore, this criterion was applied when selecting case studies, as well as for the discussion, recommendations and conclusions of this research.

The three lines of defence represents a model introduced by the Institute of internal Auditors, which elaborates on how different stakeholders fit in the wider governance framework of an organization.

Abbreviations

AI – Artificial Intelligence

AIMA – Artificial Intelligence: A Modern Approach

AGI – Artificial General Intelligence

AML – Anti Money Laundering

ANI – Artificial Narrow Intelligence

AWS – Amazon Web Services

BI – Business Intelligence

CAPEX – Capital Expenditure

CCO – Chief Compliance Officer

CIO – Chief Information Officer

CMS – Compliance Management System

ERM – Enterprise Risk Management

ERP – Enterprise Resource Planning

EU – European Union

FTE – Full Time Equivalent

GDPR – General Data Protection Regulation

ICAO – International Civil Aviation Organization

ISO – International Organization for Standardization

IT – Information Technology

ITIL – IT Infrastructure Library

KPI – Key Performance Indicator

ML – Machine Learning

OPEX – Operation Expenses

PCI DSS – Payment Card Industry Data Security Standards

RACI – Responsible Accountable Consulted Informed

RfP – Request for Proposal

SLA – Service Level Agreement

U.S. – United States

List of tables

Table of contents

1. Introduction

1.1. Setting the scene

Zora Neale Hurston, an American author and anthropologist, said “research is formalized curiosity” (Hurston, 1942). This project began as a curiosity and then it got formalized in the form of this doctoral research. It is a qualitative research that has focused on my passion for understanding the holistic picture of how people, who make up organizations, comply with the various rules and standards that are constantly imposed on them, and to understand how today’s technology enables them in this endeavour. I believe that understanding a system of compliance management is something that cannot be counted, it can be merely observed from outside, or lived from the inside. All entities of an organization will be experiencing it from their point of view, and together they will form the culture of compliance management.

Managing compliance requirements in an organization is the problem that raised the first questions, which then led to this research. Such requirements originate both from outside and inside the organization, and they are to be addressed by the various departments, functions, or units of an enterprise. The type of “compliance” within organizations is also categorized depending on the highest risks faced by an organization; hence by complying with pre-defined regulations and standards, an organization is protecting itself against those risks. This research is focused on the compliance endeavours organisations spend their resources on, to ensure risks are managed according to their risk appetite. Organizations are at the same time operating in highly regulated environments, with external governance bodies either dictating, or recommending ways to tackle compliance management. Therefore, this research is positioned within the wider corporate governance theme, and further exploring compliance management within the IT governance of an organization.

Within the business context, the topic has been normalized to take the name of a “Compliance Management System” or short “CMS”, which is what many organizations officially define within their enterprises. Since the idea of having a system to manage compliance allows for interpretations, as a system is not a physical object, organizations need guidance on how to create and how to enable such a CMS. There are numerous consulting companies today willing to step in and offer that guidance, while they position themselves as advisors on CMS design, implementation, and so on. By looking a bit further, at the influence and disruption of technology advancements on the way organizations work, the idea of understanding how the wave of automation and intelligent computer systems impacts the work that has to be done within an organization to manage compliance requirements, was sparked. Within the business context of consulting clients and guiding them based on experience, professional practice methodologies and access to a pool of subject matter experts, the rigorous research on understanding a CMS and its potential enablement by intelligent computer systems' applications was missing. This represented the driver of undertaking this research, in the pursuit of offering the practice a documented view of managing compliance across an organization in the automation era, and also to offer guidance resulting from the unique blend between practice and academia.

Therefore, the aim of this research is to provide conceptual guidelines to large organisations on deploying an enterprise-wide compliance management system enabled by AI, by investigating how CMSs are strategically set-up and to what degree they are supported by Artificial Intelligence (AI) applications, therefore contributing to knowledge as well as practice. In order to achieve this aim, five objectives were set, beginning with defining what a CMS is and critically reviewing the literature on the topics of automation, AI and CMS. The second objective was to analyse the set-up and design of CMSs within organizations by conducting multiple case study research. The third objective focused on analysing the enablers and barriers of AI adoption within large organizations. The fourth objective has compared findings from practice and theoretical underpinnings, and then explored how AI can strategically be an enabler of compliance management activities within organizations. Last but not least, the fifth objective led the research to provide conceptual guidelines, a framework for the set-up of an enterprise-wide CMS driven by AI, within large organizations.

1.2. Aim and objectives

Aim

The aim of the research is to provide conceptual guidelines on deploying an enterprise-wide compliance management system enabled by AI, by investigating how compliance management systems are strategically set-up in large organisations and to what degree they are supported by Artificial Intelligence (AI) applications, therefore contributing to knowledge as well as practice.

Objectives

1. To identify the objectives of a compliance management system within organizations by critically reviewing the literature.
2. To analyse the set-up of compliance management systems within large organisations by conducting multiple case study research.
3. To analyse the enablers and barriers of AI adoption within large organisations as part of the multiple case study research.
4. To compare findings from practice and theoretical underpinnings, and explore how AI can strategically demonstrate being an enabler of compliance management activities.
5. To provide conceptual guidelines for the set-up of an enterprise-wide compliance management system driven by AI, within large organizations.

1.3. Structure, methods and ethics

This thesis represents the culmination of this research and presents in a structured fashion, how the aim and objectives of the research were met. The thesis is organized in nine chapters, in a classic way. It starts with the present introduction chapter, followed by a definitions and theoretical background chapter, before diving into the literature review chapter. The latter is further split into key writers and debates in literature, literature review key points and gaps in current literature. The fourth chapter is the research methodology one, which is composed of the following: research philosophy, research strategy, research approach, results and findings approach, discussion of the findings approach, impact of philosophical approach on results and conclusion, originality, limitations of the current study and limitations of other research philosophies. The fifth chapter is the data collection and analysis, which elaborates on the organizational context of the case studies, how the right sample size and high quality are ensured, as well as the data coding process and analysis method. The empirical results chapter is the sixth one, being split into research propositions and connections, results from data collection and analysis, thematic structuring of propositions. To follow is the seventh chapter, the discussion, consisting of three parts: theoretical framework, discussion based on theoretical background, discussion based on thematic results and recent theory. The second-final chapter is the eight one, bringing the conclusions and limitations of this research to light. The ninth and final chapter brings up the recommendations and implications of this research. Supporting information is available in the appendices of this thesis, while explanatory information can be found at the beginning of this study, within the glossary, abbreviations and list of tables.

The research was conducted under critical realism as research philosophy, using multiple case study research as a qualitative method. Following the theory of critical realism research, the analysis of the data from the three case study organizations has been based on a coding process. This coding process represents the skeleton of this research, the theoretical framework allowing for future generalization to new cases (Yin, 1994). The categories of the coding (Appendix A) are a direct representation of the categories used in the interview questionnaire (see Appendix E). The coding was enabled by the key topic within each interview question, which led to the formulation of thirty-four research propositions as results of this study. The common attributes of the data clustered under these propositions have blended into nine themes, outlined at first in sub-section “6.3. Thematic structuring of propositions”, and further elaborated in chapter seven “Discussion”. This thematic discussion, mixed with the theoretical background and the conclusion of this research, have led to the recommended conceptual guidelines of this research, fulfilling the ultimate aim.

The qualitative nature of this research paired with the case study data collection methods used (interviews and documentation) have been accompanied by ethical approval from the ethics committee of the home university (Edinburgh Napier University). The entire data has been collected only after signed consent form has been given by the individual participants belonging to the three case study organisations.

2. Theoretical background

This chapter begins by providing an overview of the nature and objectives of Compliance Management Systems (CMS). It does so by positioning the research in the private sector and the consultancy industry. The second part of this chapter introduces key definitions related to the topic of research, before touching upon frameworks and ethics in compliance management. Some of the observed issues within compliance management are presented next, while the potential of AI in compliance management wraps up this chapter.

2.1. Legal and regulatory background

In order to set the scene as to why CMSs are necessary, this introductory paragraph provides a brief overview of what regulation is and how it influences responses by organizations (compliance). Yandle & Young (1986) make the differentiation between industry and social regulation, emphasizing the fact that social (or function) regulation is something that emerged as early as 1884. What distinguishes industry and social regulation is the legislator/regulator and client relationship. Whereas in the industry relationship there tends to be a bilateral monopoly, since regulation is addressed to a single industry target, the social/function relationship expands to multiple industries, hence it increases its scope (Yandle & Young, 1986). To help understand the puzzle of regulation at an international level, Shleifer (2005) provides an account for the evolution of the legal and regulatory regimes of countries around the world, and how it is shaped by their colonial heritage. The key regimes are originating either in (1) the English common law tradition ("independent judges and juries, relatively lower importance of statutory laws, and the preference for private litigation as a means of addressing social problems"), (2) the Napoleon-French legal system based on Roman law ("a civil law tradition, characterised by state-employed judges, great importance of legal and procedural codes, and a preference for state regulation over private litigation"), (3) the German own civil law tradition (also based on Roman law), or (4) the USSR-developed system of socialist law (Shleifer, 2005).

The context of regulation in which this paper is positioned, is the social/function one, It is such regulation that shapes the need for compliance management systems, and not just industry-focused regulation. Crafts (2006) theorizes that regulation is represented by "rules imposed by the state that constrain the actions of economic agents, typically through the imposition of standards". He also mentions that the "most obvious cost of regulation is that productive resources are used for compliance rather than to produce output" (Crafts, 2006).

Building upon this theory, it can be argued that rules are imposed not only by the state, but by independent authorized bodies as well. Organizations must comply to both industry specific rules, and to social/function rules that apply depending on the nature of business, and the jurisdiction where they operate. The different legal and regulatory regimes across the world (introduced above), will have an influence on the way corporate governance is responding, as a mechanism of control of organizations.

2.2. Nature and objectives of Compliance Management Systems

To understand how systems for compliance management came about within organizations, it is necessary to go back in time and first position CMS in the context of corporate governance and corporate controls. According to Padmanabhan (2012), corporate governance "is a process by which an institution is governed to achieve the set goals, resolving conflict of interest between different stakeholders, both internal and external." Padmanabhan (2012) also states that "governance is primarily a Board level function, managing the affairs of the company, driven top-down" to eventually "ensure ethical, legal and regulatory compliance". Considering Prowse's (1994) survey paper, it can be deduced that corporate governance is a mechanism of corporate control.

Two important institutions have marked the territory of corporate governance in the twentieth century: The Institute of Internal Auditors (IIA) and the Committee of Sponsoring Organizations (COSO). "The IIA is an international professional association that was established in 1941, with the primary mission to advocate, educate and provide standards, guidance and certifications for/to members working in internal audit, risk management, governance, internal control, information technology audit, education and security" (The Institute of Internal Auditors, 2020). The IIA has later supported the establishment in 1985 of the Committee of Sponsoring Organizations (COSO), which "came about to provide thought leadership through the development of frameworks and guidance on enterprise risk management (ERM), internal control, and fraud deterrence" (Anderson & Eubanks, 2015). COSO was formed with the purpose of sponsoring the National Commission on Fraudulent Reporting ("an independent private-sector initiative that studied the causal factors that can lead to fraudulent financial reporting") (COSO, 2020). Related to internal controls, COSO has published in 1992, the most widely known international framework, *Internal Control — Integrated Framework*. A revised and reissued version was published in May 2013, which made the 1992 framework be superseded and no longer available (COSO, 2020).

The need for officially designating compliance programs (or systems) within organizations was likely brought to public attention by the passing of the Sarbanes-Oxley Act of 2002, which demanded greater accountability by boards and top executives (Deloitte, 2017). Before this, only compliance emerged as a field, but likely not in the form of a program within organizations (Murphy, 2007). The early 2000s also saw the birth of the concept of Enterprise Risk Management (ERM), when in 2004 COSO published *Enterprise Risk Management – Integrated Framework*, which was aimed at organizations trying to better protect and enhance stakeholder value (COSO, 2017). CMSs are necessary for large organizations, as they help organize the response to the regulatory environment and support embedding ethical practices and risk management activities within daily operations. This research goes a step further, in the direction of automation and Artificial Intelligence (AI), to investigate how such technology can support compliance management across an entire organization. Before doing this, how can a Compliance Management System be defined? This question must be answered in order to grasp what the research is trying to achieve. Since the aim is to understand how CMSs are strategically set-up and to what degree they are enabled by AI applications, it is fundamental to also provide the understanding of what is meant by a CMS. A decomposition of the concept of CMS is made, and then a final interpretation of what a CMS represents is given. Earlier, the term "compliance program" was introduced. Breaking down the CMS concept in two separate parts, "compliance management" and "system", one can then see how a CMS compares to a compliance program. First, "compliance management" is composed of two nouns "compliance" and "management". This can be seen as the field studying the management of compliance, "management" implying an action. The noun "system" in a business context (Business Dictionary, n.d.) represents "a set of detailed methods, procedures and routines created to carry out a specific activity, perform a duty, or solve a problem." From the above definitions, the conclusion is, that a CMS is represented by the cumulative actions of managing compliance within a framework of procedures and routines that enable the adherence to internal and external regulations and standards that emerge from both internal and external sources. The ultimate aim of a CMS is solving the problem of addressing internal and external risks to the organisation and its stakeholders. The International Organization for Standardization (ISO) "provides guidance for establishing, developing, implementing, evaluating, maintaining and improving an effective and responsive compliance management system within an organization" through its standard "ISO 19600:2014 Compliance management systems — Guidelines" (International Organization for Standardization, 2014). These guidelines are aimed at the enterprise level and can be considered good practice when it comes to designing a CMS, hence can be used in conjunction with the recommendations of this research.

2.2.1. Private sector and consultancy industry

Firms find themselves in a constant need to comply with laws and regulations, while compliance activities go beyond compliance to external regulations, to also include compliance to internally set-up standards by the organization, as pointed out by Papazafeiropoulou & Spanaki (2016). Complexity in managing compliance within organizations is what results out of this. This research has emerged from the consultancy domain, within the private sector of business. Consultancy firms position themselves as experts in advisory services, including in addressing compliance topics. Often, the results of a survey with various top stakeholders in organisations, lead to a new offering by the consulting firm. For example, a typical offering by one of the big four consultancy firms presents in its talk book and services on "Compliance transformation" a framework consisting of eight key elements. Governance and culture represent the core of the framework, with the eight elements covering the three lines of defence of an organization: the line of business, the oversight monitoring line and the internal audit function line (KPMG LLP, 2016). This compliance transformation framework is also addressed from the angle of the internal audit function, culminating in a maturity model of the compliance transformation journey (KPMG LLP, 2017). More recent perspectives out of the consulting practice touch upon the future of regulation at its intersection with technology and society and how new technologies are disrupting regulators' work (Deloitte, 2020).

2.2.2. Compliance in a corporate environment

The noun "compliance" as a stand-alone word spans a lot of disciplines and subject areas. According to the online Cambridge Dictionary, to comply means the "act of obeying an order, rule, or request" (Cambridge University Press, n.d.-b), while compliance means "the fact of obeying a particular law or rule, or of acting according to an agreement (Cambridge University Press, n.d.-a). Elgammal, Turetken, van den Heuvel, & Papazoglou (2016) define compliance from the perspective of business processes as:

> "The process of ascertaining the adherence of business processes and applications to relevant compliance requirements, which may emerge from laws, legislation, regulations, standards and code of practices (such as ISO 9001), internal policies, and business partner contracts (e.g. service level agreements (SLAs))".

The scope of this research covers “corporate compliance”, that is the act of obeying an order, a rule, or a request, by a corporation (firm/organization). The definition to be followed throughout this study moves a step further from that of Elgammal et al. (2016), to include the adherence of not only business processes and applications (objective elements), but also of employees’ behaviour (the cultural and subjective element) and of the interaction between humans and those processes and applications. Companies have started addressing compliance as a function more predominantly after the year 2000, when corporate accounting scandals have made the highlights of the news. Papazafeiropoulou & Spanaki's (2016) list of existing literature on Governance, Risk and Compliance systems starts with the year 2004. This is in line with the search for literature on “what is corporate compliance”, which brings scarce results, but one paper from 2004. As such, in his 2004 paper, Willging (2014) explains that:

> “Corporate compliance consists of those policies and procedures that govern the operations of the entire enterprise in accordance not just with all known legal responsibilities, but with the highest standards of professional and ethical conduct.”

Important to take away from this definition, is that the means to achieving compliance are represented by policies and procedures applicable to the entire organization, addressing not only external responsibilities (legal and regulatory), but also internal ones (standards of professional and ethical conduct). Furthermore, this definition also emphasizes that compliance is driven by an ethical behaviour, therefore the culture of a corporation should cultivate this behaviour. More on ethics within compliance management will be covered in the section to come. Murphy (2007) mentions that the idea of compliance within organisations as a separate field started in 1991, and since then it has emerged into compliance programs. These programs are actually addressing a variety of risks that organizations are facing, by establishing a proactive approach to unavoidable issues. In these early stages of defining corporate compliance, basic elements of a corporate compliance program were listed by Willging (2014), namely:

- The organization must define and document acceptable standards of conduct and ethical behaviour.
- Staff must be trained to adhere to these standards.
- An internal review and audit protocol must be implemented.

The above elements do not specifically mention whether this program touches on compliance with both external and internal regulations and standards. It can be assumed that acceptable standards of conduct and ethical behaviour encompass those standards referring to the adherence to, and of, business processes and applications.

2.2.3. Enterprise Compliance Management System

The wording "enterprise compliance management system" appears in one short article (Williams, 2005) and is not addressed in literature as a concept per se. Another reference has been found in Butler & McGovern (2012), where Hayward's (2007) paper *"Enterprise Compliance Management Systems (ECMS): choosing the right system and the real costs involved*" is documented. Furthermore, some of the previous studies investigate Enterprise Management Systems and describe how such systems offer an integrated approach to tackling management relevant topics, amongst which compliance management is one (Lux, Hess, & Herterich, 2013). Another article discusses ideas for the implementation of enterprise wide compliance management powered by semantics of policies, and it addresses the concept of "enterprise compliance management", culminating in an approach on automating the compliance checking process of emerging policies (Kharbili, Stein, Markovic, & Pulvermüller, 2008). The idea of ECMS is addressed further in this study, as the aim is to offer guidelines to organizations to deploy an enterprise-wide compliance management system. ECMS is not studied as an IT system, nor looking only at emerging compliance processes (but also at adherence compliance processes), rather as a "system" as defined in this paper (see definition under Compliance Management System).

2.2.4. Governance, Risk and Compliance

Governance, Risk and Compliance (GRC) is a function within organizations, a subset of which is compliance management. GRC is part of an organization's corporate governance and will differ in the way it is organized to respond to compliance management, depending on the legal and regulatory regime it operates in (see section 2.1. above). To emphasize this, it is worth understanding the difference between European Union's (EU) and United States' (U.S.) approach to corporate governance. In the EU, the comply-or-explain principle is the central element of most codes of corporate governance (Sturm, 2016). Originating in the UK in 1992, the comply-or-explain principle was put forward by the Cadbury Committee "as a practical means of establishing a single code of corporate governance whilst avoiding an inflexible 'one size fits all' approach (Seidl, Sanderson, & Roberts, 2009). In contrast to the comply-or-explain principle, in the U.S. corporate governance is put into force mainly through rule, such as through the Sarbanes-Oxley-Act (Sturm, 2016). Therefore, GRC functions of organizations with international operations, are expected to have flexible approaches, to satisfy the different principles of the code of corporate governance, within different countries.

The GRC concept per se has been first referred to in the corporate world around 2004, given that the search for scholarly, peer reviewed literature, using the key words "governance risk and compliance", yields results from 2006 only. PricewaterhouseCoopers (PWC) has published in 2004 already, an operational model for GRC (as listed by Papazafeiropoulou & Spanaki (2016)), yet, only in 2006 the first studies on the topic have appeared. While the GRC concept is mostly addressed in literature from an information systems perspective, Tadewald (2014) describes it as a critical business concept, integrating a risk-based management approach to governance that is proactive, effective, and that can be used throughout an organization:

> "It provides organizations with a uniform view of information so it can align risk management with objectives, reduce complexity, diminish inconsistencies, and harness technology for desired outcomes. Not a replacement for internal control or compliance testing, GRC goes well beyond testing to create a comprehensive framework for managing risk and improving performance. It organizes risk management efforts rather than duplicating them, which reduces overall operating costs and assists in creating a more risk-intelligent organization."

This explanation provides the link to the subset of compliance management, since, as mentioned in the definition of CMS, its purpose is to address internal and external risks to the organization and its stakeholders. Subsequently, an organized approach to risk management will support the system of managing compliance to address the right risks across the enterprise, hence the need for an enterprise-wide compliance management system (ECMS).

2.3. Frameworks on compliance management

Existing frameworks and concepts related to compliance management are depicted in this section. Firstly, the "three lines of defence" model of organizational structure is introduced as a framework, to understand responsibilities of different stakeholders of an organization in responding to risks and compliance. Next to the three lines of defence, the four commonly referred to pillars of corporate governance are introduced, to highlight the overlap between an organisation's lines of defence and its corporate governance. Secondly, the concept of "Enterprise Risk Management" is presented as an overarching set of organizational culture, capabilities and practices embedding compliance management. Thirdly, there is a discussion of embedded ethics in the management of compliance activities.

2.3.1. The three line of defence

The “three lines of defence” is a model introduced by the Institute of Internal Auditors, which elaborates on how different stakeholders fit in the wider governance framework of an organization. As the name says it, the model is based on three “defending” lines, which are meant to address the risks faced by the organization, in the sequence of the numbering. Hence, the first line, composed of the business lines, is the first one responding to risks by adopting management controls and other internal control measures. The second line consists of various support functions (financial control, security, risk management, quality, inspection, compliance), which are ultimately responsible for providing the necessary tools and support to the first line of defence, in order to address risks in a sustainable way. The third line is represented by internal audit, which is independent from management as a function, and whose role is to provide assurance on the effectiveness of governance, risk management, and internal controls, reporting to the board of directors (The Institute of Internal Auditors, 2013). The “three lines of defence” model is used within this research to understand how a compliance system is embedded within each of these three lines of the case study organizations. Furthermore, it is used as a discussion framework for the findings of this research.

The role of the Board of Directors is monitoring the effectiveness of the internal audit function and the assurance it provides (Chartered Institute of Internal Auditors, 2019). Per se, the board resides outside the three lines of defence of the organization, because it is not directly involved in “defending” the organization. Instead, the board of directors represents the overarching power (together with Senior Management), steering the way in which the lines respond to risks and opportunities to protect the organization and help it achieve its objectives. Given this role, this research builds up its recommendations based on the three lines of defence model to include also the oversight role of the board of directors in this framework. This is in line with the concept of the four pillars of corporate governance (the management, the board, internal audit and external audit). In addition, Arndorfer & Minto (2015) introduce the concept of the “four-lines-of-defence” (for the financial industry), where external audit and the regulatory supervisory bodies together form the fourth line of defence of an organization. The external parties in the fourth line of defence are, according to Arndorfer & Minto (2015), a vital element of assurance and governance systems.

2.3.2. Enterprise Risk Management

It was mentioned before that the ultimate aim of a CMS is solving the problem of addressing internal and external risks to the organisation and its stakeholders. Responding to identified risks and introducing the appropriate control activities is the responsibility of management, which should establish and implement the right policies and procedures. Therefore, it can be deduced that by being compliant (to both internal and external policies and procedures), an organization is managing its risks. When this is orchestrated across the entire organization, it can be assumed that management has deployed enterprise risk management practices.

The early 2000s saw the birth of the concept of Enterprise Risk Management (ERM), when in 2004 COSO published *Enterprise Risk Management – Integrated Framework*, which was aimed at organizations trying to better protect and enhance stakeholder value (COSO, 2017). This framework was updated in 2017 by the "Enterprise Risk Management–Integrating with Strategy and Performance" release, "which highlights the importance of considering risk in both the strategy-setting process and in driving performance" (COSO, 2020). ERM can be defined as "the culture, capabilities, and practices that organizations integrate with strategy-setting and apply when they carry out that strategy, with a purpose of managing risk in creating, preserving, and realizing value" (COSO, 2017). Among the culture, capabilities, and practices, are activities related to the management of compliance requirements, which in turn help respond to that risk to support the creation, preservation and realization of value across the organization. By merging the two concepts of CMS and ERM, it can be deduced that a system of managing compliance across the organization, is a core enabler of the ERM endeavours, therefore supporting the system of monitoring, learning, and improving performance (COSO, 2017) within an organization.

2.3.3. Embedded ethics in compliance management

A key strategic decision in adopting a compliance management system should be deeply informed by ethical considerations. Pérezts & Picard (2015) argue that risk assessments and compliance with regulations are human activities requiring intuition in analysis and evaluation, and therefore will be influenced by the ethical judgement of those individuals. This 2015 ethnographic study is conducted within a single organization, and it highlights the behaviour of people in the process of decision making related to regulated activities. Such topics belong to the culture of the organization since acting ethically and with integrity is something employees live on a daily basis within their work environments. To accentuate this Sheedy, Zhang, & Tam (2019) find that "personal attitudes to risk management/compliance matter in risk compliance behaviour", and that in an ideal such organizational culture, frequent communication of the importance and the benefits of compliance with risk policies, is paramount. Later in this research, the concept of ethics of Artificial Intelligence (AI) is briefly addressed as part of the "governance of AI" topic, since ethics are a core part of not only activities in human-driven compliance management processes, but also in the design, rules, and algorithms built within AI applications that enable those processes.

2.4. Issues within compliance management

The next section indicates some of the issues organizations face when dealing with the topic of compliance management systems within their environments. These issues are on one hand the difficulty of efficiency measurement of compliance management activities, and on the other hand dealing with isolated ways of managing compliance requirements, or silo compliance activities. Important to note, is that these do not represent an exhaustive list of issues but are topics that have partly sparked the aim of this research.

2.4.1. Measuring efficiency of compliance activities

Achieving efficiency is probably one of the most sought-after goals of organisations. As a general statement, it has a connotation that implies doing things right, with minimum efforts (resources, time etc.). Management efficiency is researched by Pawłowski, Piatkowski, & Żebrowski (2009), who study the three-efficiency-levels approach (organization level, process level, workstation level). These three levels can be directly mapped to the three lines of defence: first line equals workstation level, second line equals process level, and third line equals organization level (under the limitation that the third line represented by internal audit is independent from management and operations, only providing assurance across the organization). From this paper, the core element to take away is that efficiency within a company has to be not only defined as a term, but rather based on its measurement. Efficiency is, therefore, an interactional process, which encompasses phenomena taking place inside of an organization, as well as between the organization and its surroundings (Pawłowski et al., 2009). The outcome of these interactions leads to certain results, which an organization typically measures using company economic efficiency ratios split in four categories: (1) operating efficiency (return on sales, profit margin, payback period, turnover of capital employed, fixed capital investment ratio), (2) liquidity (debt ratio, equity to fixed assets ratio, fixed asset ratio, current assets self-financing ratio, current ratio, assets liquidity ratio, net assets), (3) profitability (fixed capital structure ratio, return on capital, financial costs ratio, return on equity), (4) market ratios (nominal value vs ordinary share, earnings per share, dividend per ordinary share, dividend ratio, return on share) (Pawłowski et al., 2009). Horne (2016) sustains this view and says that organizational efficiency is measured through a number of economic artefacts. Yet, given the difficulty in quantifying costs and allocating direct return (e.g. supported revenue) to compliance activities, these economic ratios of measuring efficiency are not ideal to use in this case. Another ratio of economic efficiency, that does not belong to any of the four categories above, but rather drives the strength of them and could also be a good metric for management, is represented by the so-called "return on compliance". Research on the topic of setting a formula on how to calculate return on compliance is on-going, but still lacks any maturity or testing of usability, with examples such as Nso's (2019) equations for return on compliance investment and return on capital employed in a compliance program. The potential here is to appraise compliance management systems based on output rather than costs, and therefore shift the general perception of compliance to it being a cost centre as opposed to the current view of it being a profit centre (Nso, 2019). Following Horne's (2016) proposed framework, efficiency is defined by the foundational equation "resources = requirements", and considers that management's role is one of continuous refinement in reducing the costs of resources (what is consumed) to meet business (client) requirements (to produced what is required). Therefore, the achievement of efficiency through compliance management should consider the balance between resources and requirements (compliance requirements and requirements of the core business of the organization). The data collection of this research has consequently attempted to gather information about what type of resources are consumed by an organization to run a compliance management system.

2.4.2. Silo compliance

The purpose in bringing up silo compliance is to highlight the issue of compliance often being an isolated exercise within organizations, rather than a subject addressed across the enterprise. This is a statement based on the experience made in working with clients within the consulting practice. It is important to address, as the scope of this research covers the management of compliance as a system across an organisation, and not individually within a department or function. At the same time, the complexity of compliance management cannot be reduced by simply isolating the different types of compliance (external laws and regulations vs. internal standards and practices). To shed light on the above statements, two representative examples of types of silo compliance within the implementation of IT tools in organizations are given. These are examples easy to grasp as they refer to concrete software that support the management of compliance related topics:

- One system compliance (e.g. implementation of an Enterprise Resource Planning (ERP) system across the organization).
- Multiple systems compliance: with no integration between systems, no overall picture and hence no overall governing strategy of systems (e.g. implementation of various systems that each allows individual compliance with one or more rules/laws/standards). The implementation in such a case only partly reconciles with other business processes and therefore does not belong to the idea of an "enterprise compliance management system" (ECMS) (see definition under Enterprise Compliance Management System).

The search in literature for "silo compliance" yields an isolated result, where the term is referred to as compliance "efforts scattered throughout business silos" as opposed to holistic compliance (Volonino, Gessner, & Kermis, 2004). The topic of silo compliance as scattered efforts has been addressed in the case studies' data collection phase, in order to investigate and analyse how organizations deal with this in the set-up of their compliance management activities, thus supporting the achievement of objective number two of this research.

2.5. The potential of AI in compliance management

The field of Artificial Intelligence (AI) arguably dates back to the 1950s. This is when the term has been used at a summer conference at Dartmouth College, in Hanover, New Hampshire (Bringsjord & Govindarajulu, 2018). Not surprisingly, there are a lot of definitions attempting to articulate what AI is, while many fail to provide a simple, logical clarification. Russell, Norvig, & Davis (2010) explanations from their book "Artificial Intelligence: A Modern Approach (AIMA)" to what AI is, shall be used to denote how AI is explained within the context of this research. Russell et al. (2010) say that AI is primarily two-folded: (1) Human-based – systems that think and act like humans and (2) Ideal rationality – systems that think and act rationally. Here the split is also done on reasoning and behaviour (see Table 1).

Table 1. Four Possible Goals for AI According to AIMA (Bringsjord & Govindarajulu, 2018)

	(1) Human-based	**(2) Ideal rationality**
Reasoning-based:	Systems that think like humans.	Systems that think rationally.
Behaviour-based:	Systems that act like humans.	Systems that act rationally.

If AI is represented by computer systems, then this research becomes one where the aim is to find how human-based and ideal rationality computer systems can drive a compliance management system. Ultimately these computer systems will be having the characteristics, on one hand to act like humans, and on the other hand to act rationally.

With the attempt to explain AI as a human-based, respectively ideal-rationality computer system, it is worth introducing two core subfields/types of AI. Others (Farrow, 2019) indicate more than six sub-disciplines of AI, but the view of this study and for the sake of simplicity, the two ones mentioned below, cover the two basic ways in which AI is used today.

- The first type is known as Machine Learning (ML). The growth in AI applications has been made possible through the development of new algorithms, which support any application by improving the performance of a task through capturing the ideal performance of that task through a learning loop, a repeated experience of the task – this is what ML is (Bringsjord & Govindarajulu, 2018). ML algorithms are used in speech and text recognition systems, spam filters, online fraud-detection systems and product-recommendation systems among other applications (Bringsjord & Govindarajulu, 2018).
- A second type of AI is known as symbolic AI, which is represented by rule-based applications that rely on a structured representation of human knowledge provided to the algorithm by a subject human expert (M. Ferrini, personal communication, 2019).

Ng (2019) proposes another angle for splitting AI in two types: Artificial Narrow Intelligence (ANI) and Artificial General Intelligence (AGI). ANI is represented by applications run by computers systems that can do one task only, such as smart speaker, self-driving car, web search or face detection. On the other hand, AGI is represented by computer systems that can do anything a human can do in a certain field, or even be super-intelligent and do more things than a human can (Ng, 2019). AGI will need a lot of technological breakthroughs before becoming a reality (Ng, 2019). Hence the focus today and in the foreseeable future is on ANI.

Augmented Intelligence instead of Artificial Intelligence is probably a more down to earth naming convention and therefore it should be understood that through AI, this research is looking at how applications are automating certain tasks previously undertaken by humans, either through ML or symbolic AI, and therefore these applications represent an augmentation of the human intelligence, where systems inform the human and do not replace her/him. This view is sustained by Farrow's (2019) paper, where she introduces the advancements of the period 1990-2010 as relating to the augmentation of human decision making (through e.g. speech transcription, text translation, face recognition) to an extent to be used in real-life applications, and to the maximization of the vast availability of data sources.

Gaining from the previous definitions, the scope of this research is to explore and analyse a system as a framework of procedures and routines, hence explain how these can be embedded in or supported by AI applications/algorithms (procedures and routines of their own) for driving a system of compliance management. Since AI algorithms are nothing else than procedures and routines of their own, the compliance management mind-set has to sit behind these as well. Compliance management for AI applications is a complex topic, and is briefly addressed further on in this chapter, under the section "debates in literature".

3. Literature review

This chapter begins with a reiteration of the importance of corporate governance to the subject of compliance management systems, and then introduces the sub-section of IT governance. The latter is setting the scene for one of the key debates presented in this paper, that of "governance of Artificial Intelligence". The review of literature continues with the key debates, and the influential models. Completing the chapter are notes on the gaps in current literature, which are being addressed by this study.

3.1. Corporate and IT governance

Based on the definition introduced by Padmanabhan (2012), governance is the board's responsibility and one of the key objectives is ensuring ethical, legal and regulatory compliance. Weill & Ross (2004) articulate a framework that specifies that "the board works with a senior management team to implement governance principles that ensure the effectiveness of organizational processes", which in turn must ensure compliance. Already at the beginning of the century Weill & Ross (2004) introduced the importance of IT governance under the umbrella of corporate governance, defining IT governance as the act of "specifying the decision rights and accountability framework to encourage desirable behaviour in the use of IT". Furthermore, they explain the simple fact that "governance determines who makes the decisions, while management is the process of making and implementing the decisions" (Weill & Ross, 2004). Within IT governance, the global organization that provides the standards for information governance, control, security and audit professionals, is ISACA (ISACA, 2021). Known originally as the "Information Systems Audit and Control Association", it was formed in 1967, while in 1976 it has formed an educational foundation responsible for large-scale research in the areas of IT governance and control fields (ISACA, 2021).

3.2. Philosophies, debates and themes

To emphasize the validity of the research approach, this section starts with a quick overview of the key philosophies in existing literature. It then continues with the debates and main themes identified in the current body of knowledge.

3.2.1. Research philosophies in literature

The existing literature on the topic of compliance programs and systems is conducted using a variety of methods, from Abdullah, Indulska, & Sadiq (2016), Gozman & Currie (2014) and Kumar, Pollanen, & Maheshwari (2008) multiple case study approach, to descriptive articles that rely on narrative discourse (Murphy, 2007; Tadewald (2014); Sadiq, Governatori, & Namiri (2007); Boland (2006); Ramanathan, Cohen, Plassmann, & Ramamoorthy (2007); Sammer (2005). A few studies are conducted using a quantitative method, such as Parker & Nielsen (2009), Knuplesch, Reichert, & Kumar (2017), Elgammal et al. (2016).

The review of literature indicates predominance in using the case study method in researching how compliance is managed within organisations, with examples of ethnographic studies such as Pérezts & Picard (2015). This is likely to be so because the topic is a fairly subjective one, with peculiarities applicable to each individual organization. Generalization is done at the framework elements level. Statistically, it is likely to be difficult to demonstrate the generalizability across industries and organizational size.

3.2.2. Debates in literature

To enable a more focused critical discussion of previous research, the reviewed literature is here split into six main categories, based on the dominant subject of analysis: business process compliance management, compliance management audits, compliance information systems, risk-based compliance, corporate compliance systems and governance of Artificial Intelligence. The categorization process informs the literature review theory, which is used in the “Discussion” chapter. A comprehensive list of key writers to the subject of research has been summarized in a tabular form and can be found in Appendix H of this paper.

1) Business process compliance management

Elgammal et al. (2016) use an own developed software tool (Business Process Compliance Management Tool Suite or BPCM) to study the design-time compliance management framework on two case studies in two different industry sectors. Elgammal et al. (2016) argue that it is paramount to take a preventive focus in compliance management; hence enforcing compliance by design is a first step towards compliance support. Elgammal et al. (2016) also recognize that many software vendors have introduced commercial products that combine a set of compliance solutions, but that in effect are highly proprietary and technology-specific. Their BPCM tool can be argued to be bias-free, as it is employed for this particular study and not for the purpose of selling it under license to as many organisations as possible. The conclusions of this study also sustain this bias-free approach, as they highlight the fact that social and organizational aspects are as important as formal methods (using computer science, business process management, legal studies). The key take-away is that business process compliance cannot be fully automated by applying only compliance patterns (in the form of algorithms), as it will always require an element of human judgement and intervention. Ideally, the recognized compliance patterns that are translated into formal compliance rules within a company-wide BPCM are supplemented by employee actions that work complementary forming an overall compliance management system. Kim & Kim (2017) show through their research, that this take-away is valid, as they study both active and passive IT utilization groups of employees. They conclude that compliance behaviour is mediated by compliance knowledge because it fosters voluntary compliance.

Another study looking at business process compliance, is that of Knuplesch et al. (2017). The main argument of this paper is that compliance cannot be completely ensured at design time, and should therefore be part of a continuous monitoring process. Knuplesch et al., (2017) introduce a framework based on visual monitoring of compliance activities performed along the execution of a process. This study is designed to empirically demonstrate, through the use of an extended Compliance Rule Graph and algorithms for visual markings, how users can monitor business process compliance and ensure the continuation of “should-be” activities. An obvious limitation of relying on such an empirical framework is the negligence of human factors within the process’ activities in scope.

Compared to Knuplesch et al. (2017), Elgammal et al. (2016) address business process compliance where the focus is actually fixed on the time of design of the compliance rules that are enacted in a process, based on identified compliance patterns. It can be fair to assume that these two studies complement each other, forming a chain of solutions for business process compliance, starting with the design phase, and moving to the monitoring of compliance activities. Yet, Knuplesch et al.'s (2017) paper is restrictive, since its conclusions are drawn from the analysis of one business process only (that of hiring in a human resource department). Therefore, the validation of the proposed framework cannot be accounted as complete, further business processes should be analysed.

2) Compliance management audits

In contrast to the proactive approach to compliance management discussed above, auditing compliance requirements represents a reactive approach. Ramanathan et al. (2007) discussed in their paper, the role of audit logs for compliance management. These audit logs help demonstrate the enforcement of compliance in an organization's IT infrastructure (including IT controls that meet IT compliance objectives). They are hard elements in a control phase, helping build the trust in information systems. These information systems support the duty of processes to be compliant with company-defined regulations and standards.

Butler & McGovern (2012) go into a niche of CMS, while addressing environmental regulations and standards. Their most important argument is that to ultimately define a CMS architecture, there has to be a way to solve issues related to, firstly, knowledge management problems (complexity and scope of the global regulatory environment), and secondly to data and information management problems (actual business operations data). In the latter case, information asymmetry between different stakeholders the organization has to deal with, is hard to address within an information system. Hence, the mapping of all regulatory requirements to data from business operations and then the logical linking of these two, is not an easy to implement solution. Should there actually be an information system available to support these requirements, performing audit procedures to check the fitness and accuracy of the system, would be a fundamental element of a CMS. Therefore, Ramanathan et al.'s (2007) arguments for the role audit logs play in managing compliance, are supported by Butler & McGovern's (2012) research on interlinking knowledge management and information management for a better CMS architecture.

3) Compliance information systems

As already seen in the studies examples above, the information systems perspective on CMS appears quite often in literature. In contrast to these, Kim & Kim's (2017) study of compliance behaviour in information systems, has empirically demonstrated how two elements are highly necessary for putting an effective compliance program into practice: (1) a culture and infrastructure of compliance, and (2) a compliance IT system. The strong feature of this study is that it investigates the actual usage of information systems (and not its design and functionality to support compliance), by classifying users in active and passive groups. The results are aimed at supporting companies in developing, not the CMS, but compliance support systems. The interlinkage between these systems and, as already described by Butler & McGoverns (2012), the mapping of standards and regulations to it, can be considered pivotal in defining a CMS architecture. Kim & Kim (2017) paper beautifully presents the limitations of the research, keeping the findings in context and providing a great emphasis on the factors that must be taken into account for validating the conclusion of the necessity of coexistence of the two elements of an effective compliance program. Gozman & Currie

(2014), look in more depth at the implementation of such compliance IT systems, in the financial sector. They come to the conclusion that tight deadlines for implementation set by regulators, can negatively impact the organization by not allowing it to focus on more than meeting those deadlines, hence missing the chance to develop a strategic, enterprise-wide compliance program. Such a scenario can lead to silo compliance exercises, which end up being isolated from the rest of the organization due to high pressure of meeting the scheduled deadline of "go-live". In the area of compliance information systems Sesen, Suresh, Banares-Alcantara, & Venkatasubramanian (2010) propose an IT system solution that supports compliance to regulations, with a study from the pharmaceutical industry (a tightly regulated industry and with fairly easily definable steps in research, development and manufacturing processes). Coming up with an ontological representation of domain rules in a machine-understandable format, the study suggests that an automated system can embed regulatory requirements and support decision-making (Sesen et al., 2010).

4) Risk-based compliance

The concept of risk-based compliance is predominantly studied within the financial services industry. Some findings state that small financial institutions are less prone to implement a risk-management approach to compliance management (Gabbi, Musile Tanzi, & Nadotti, 2011). In the banking sector, Haynes (2005) argues that risk-based compliance can only work as an overarching exercise, integrated across the entire enterprise, and being part of a proactive compliance programme. Somehow on these argument lines, lay the results of Pérezts & Picard (2015), who find that personal ethics of those interpreting and responding to regulation are creating the "comfort zone" of a compliance program, since these agents are ultimately making the decision based on the risks that regulation addresses. Others have looked at technology-enabled compliance management, criticizing the reliance on tool-based GRC decision making (Bamberger, 2010). The latter indicates that such tools are prone to disable to human judgment in identifying, assessing and ultimately managing risks, which can lead to non-compliant activities. Another view along the lines of risk-based compliance management is found in Müller & Supatgiat (2007), a study researching how a risk-based model is the best approach to "optimally selecting, prioritizing and implementing appropriate compliance measures, and also determining the optimal inspection policy". This paper points out that an organization's risks drive which compliance measures are selected and applied. Overall, there is a need to incorporate the understanding of risk-based compliance within organizations, to determine if the measures employed are feasible and aimed at minimizing the total cost of compliance (acting upon measures, inspecting/auditing, implementing outcomes).

5) Corporate compliance systems

Moving away from business process compliance management, compliance management audits, compliance information systems and risk-based compliance there are other areas explored in literature. These focus more on compliance as a function and how this function is integrated in the business as such. Yet, the available literature is scarce, since most literature focuses on designing process compliance, missing the top level, management view.

From this perspective, highly regulated industries have been extensively studied. For example, the pharmaceutical industry is one of the most regulated in the world, which makes is it a perfect candidate for introducing compliance management systems that address the regulatory maze. In a 2010 commentary paper, Pluta & Poska (2010), discuss the benefits of introducing an organized approach to address pharmaceutical compliance. The approach is based on the concept of compliance by design (CbD) and a compliance master plan (CMP), where the design and its principles are documented. These approaches and methods to improve compliance management are spun out of the pharmaceutical manufacturing best practices, and evaluated to uncover their applicability to compliance. Although the paper proposes a structured approach with listed elements as part of CbD, the path of deriving these results is not backed up by rigorous research methods. Since this paper has not been written in the context of an academic setting, the proposed solution can only be considered to a certain extent. Overall, Pluta & Poska (2010) have provided through this paper valuable insights into how to structure and document compliance activities. Furthermore, these insights could be coupled with Elgammal et al.'s (2016) findings, for an investigation into how theoretical elements of a structured CbD model can be embedded as functional requirements into a BPCM tool.

To counterbalance the reduced reliability of the findings discussed above, Parker & Nielsen (2009) provide a robust study where the focus is on management of compliance, rather than design, touching on the behavioural aspect of those charged with the responsibility. Their empirical study concludes how a formally structured CMS can translate into practical compliance management; achieving enterprise compliance requires however elements such as compliance values, managerial oversight and planning, and organizational resources. This conclusion is very important, and also reliable, since the study included a large population of

999 businesses. Nevertheless, the limitations are found in the geographical distribution (only Australia), and the limited type of compliance (competition and consumer protection law).

A very interesting analysis of the behavioural economics of compliance systems is written by Langevoort (2002), who says that "compliance is indeed a struggle, with no simple check the box solution". Throughout this analytical paper, Langevoort (2002) provides clear arguments on why it isn't as easy to just tick a box to implement and demonstrate compliance, due to the struggle to find balance between the first line supervision and second line of compliance authority (e.g. auditors). Langevoort (2002) argues that most compliance systems are monitoring-based (using professional auditors), implying very high costs for the organization. Line supervision is on the other hand prone to predictable heuristics and biases (Langevoort, 2002), as well as to self-discipline and integrity, hence very subjective factors. Looking at both the analysis of Langevoort (2002) and Parker & Nielsen's (2009) study, it can be deducted that indeed an enterprise compliance system requires a thorough understanding of its costs and benefits, and subsequently it requires a fine allocation of organizational resources between instituting the right corporate compliance values (first line of supervision) and charging managerial authority with oversight responsibility.

Parker (2003) furthers the research on the role of audits, to look into audits of corporate compliance programs. These audits differ slightly to the second line of compliance authority mentioned above, since they represent a management review of the compliance endeavours across the organization. The key take away from Parker's (2003) study is that the product of the audits is a report addressed to management on how they can improve the system of compliance, but that it has little effect on the regulators, since it does the job of simply providing a statement of assurance (a tick the box exercise). What this tells us is that no matter how elaborate and advanced an organization's compliance program is, it will not spark any rethinking of laws and regulations from the regulators' side. This is due to the limitation of the communicative energy in the typical compliance program audit (Parker, 2003).

6) Governance of Artificial Intelligence

The governance of Artificial Intelligence (AI) is perhaps a topic that has been overlooked by companies over the past decades, while the field has advanced in technical development and while more and more AI applications have been deployed within organizations. Going back to the beginning of the literature review chapter, governance of AI belongs to an organization's IT governance, which is part of the overall corporate governance (a function of the board). At the same time, the control and assurance of AI go beyond the work of traditional auditors, and are topics researched and addressed by ISACA. Research on benefits and ethical concerns of automation start to appear, such as the one applying stakeholder theory to automation (Wright & Schultz, 2018). The latter rightfully argues that regulation and oversight have to be embraced by organizations when it comes to AI governance, since currently minimum legislation exists to regulate automation, and therefore an effective governance in this area still needs a lot of steps to be taken (Wright & Schultz, 2018). Governance of AI is also seen as an opportunity, arguing that the quality of information available to support decisions, is improved (Dwivedi et al., 2019). Probably before or even in parallel to developing new legislation, a closer attention should be given to the concept of explainability of AI. Barredo Arrieta et al. (2020) introduce the concept of “Responsible AI”, which is rooted in the emerging need to understand how decisions are furnished by AI methods because systems using AI ultimately affect human lives. “Responsible AI” is a methodology that encompasses fairness, model explainability and accountability, and provides a detailed taxonomy that can serve large-scale implementation projects of AI applications in organizations (Barredo Arrieta et al., 2020). Eventually, being equipped with the right understanding of the backend of AI applications, and at the same time having the legislation in place to regulate AI-driven processes is what is needed by a governance programme of AI. Ultimately, this gives a level of control on AI applications by demonstrating compliance to sound policies/legislation/standards and hence reduces the risks posed by AI-driven processes, enabling processes at their own end to be compliant. The control of AI applications must also consider the embedded ethics within the design of such applications. As earlier introduced under “definitions and theoretical background”, ethical considerations are driven by the culture of the organization, and compliance with risk policies is encouraged through frequent communication (Sheedy et al., 2019). In the case of AI applications compliance with risk policies, this communication has to consider the dissemination of information to the stakeholders on how such applications embed ethics within their design, hence are compliant by design.

Another key consideration in governing AI is deciding the type of AI organization desired on a strategy level. According to a Workera (n.d.) report, there are three types of AI organizations: the data science organization, the machine learning organization, and the hybrid of the two. The data science organization’s scope is to have actionable insights, with workflows including data collection, analysis and suggestion of actions (Workera, n.d.). The scope of a machine learning organization is to automate tasks in order to decrease operational costs or to scale a product, with workflows including data collection, models training, and models deployment (Workera, n.d.). The type of AI governance considerations to be given to these types of organizations differs, therefore it is important for organizations to have a clear strategy regarding their ambitions with AI.

3.3. Literature review key points

The literature review has led to clustering existing papers in a few categories: business process compliance management, compliance management audits, compliance information systems, risk-based compliance, corporate compliance systems and governance of Artificial Intelligence. Furthermore, throughout the process of reviewing and identifying the literature that supports the achievement of the first objective of this research, it has been seen that the topic of compliance is not hard-coded, and it pertains many subjective facets. In this summary, such subjective aspects are classified either under reactive or proactive compliance management.

3.3.1. Reactive compliance management

The reactive part of compliance, such as conducting audits (on one hand audits of internal processes, on the other hand, audits of compliance programs), looks at identifying areas of good compliance and also non-compliance, and at overall fit-for-purpose status of compliance activities. Parker (2003) presents a depiction of the compliance program audit chain of accountability in her 2003 paper, where she outlays the findings from her research on the Australian Competition and Consumer Commission and Australian Securities and Investments Commission. The benefit of these results is the fact that it supports the understanding of how the audit report is linked to management, which in turn is responsible for the compliance program, and which ultimately impacts the corporate performance and therefore the compliance outcomes. Parker (2003) suggests enriching the chain by creating loops in the communication of audit results between management and regulator, and not just pushing the audit report to the regulators as a mere statement. This is indeed a fact that is often encountered in the audit world, be it compliance program audits, or statutory financial audits. The key problem is that once there is an issue that breaks out, investigation of causes may reveal aspects that could have been addressed proactively, should the audit report be thoroughly analysed in a discussion panel including the auditor, the regulator and management. Remaining in the area of audits, another angle to discuss is the monitoring of the optimal level of compliance by an organization. Looking at behavioural economics of corporate compliance, Langevoort (2002) argues that there certainly are benefits provided by third party audits on the level of compliance within organizations, yet he explains how calculating the costs proves to be a challenge. Langevoort's (2002) view is well substantiated in this article, with very logical argumentation, including elaborating on how professional auditors are prone to a diminished ability to find risk factors that need follow-up. Particularly interesting is the fact that human monitoring is using cognitive shortcuts to cope with the vast amount of data required to be processed. This opens up the question whether or not compliance management could and should be supported by technology, and AI. Organizations can move away from reactive compliance management, to adopt a proactive approach by using AI applications, which can deal with the vast amount of data and which can easier predict risks.

A further topic addressed earlier in the review, is that of silo compliance. There are various elements of what constitutes silo compliance. For example certain IT implementation programs represent compliance exercises, which end up being isolated from the rest of the organization due to high pressure of meeting the scheduled deadline of “go-live”. Another example is the comfort zone that is easily reached by employees expected to perform compliance management activities within their own area. This comfort zone can even give birth to reactive compliance, because anything that lies outside daily habits/routines is not being picked up. Reaction is inexistent until something actually happens and triggers the need for compliance.

3.3.2. Proactive compliance management

In a world where compliance to regulations and standards is predominantly reactive, the habit of proactively taking on the challenges and costs associated with complying has to be trained. Voluntary compliance is rarely observed, because reaching that state of maturity where organizational values promote and sustain anticipative actions, is often second priority to boards. It is also a question of ethical considerations that should be embedded in the lived compliance management culture of organizations, as seen from studies such as Pérezts & Picard (2015). The size of an organization also plays a key role in this approach. Size will affect the risks that the CMS has to deal with, where large organizations are expected to deal with risks more efficiently, but also have far more risks to address. AI can be an enabling partner in achieving the state of proactive compliance management, by tapping on its ability to deal with large amounts of data, data sources, learn from the past and predict future outcomes, rather than just forecast. At the same time, organizations can tap on AI’s capacity to perform routine compliance tasks that leave time for humans to go the extra mile in achieving high compliance management maturity, where human intuition and sensibility are required.

The next challenge to overcome is governing AI. This opens up yet further questions for consideration within this research, and potentially future research: in a world governed by algorithms, how is the governance of algorithms addressed? How does the AI-driven CMS ensure AI is complying at its own level with what it should comply? How can the data produced by AI systems be trusted? Will the audit world develop fast enough to be able to audit algorithms? Being able to think about these challenges and demonstrate that governance of AI is addressed in the CMS represents a proactive habit of a mature organization. At the same time, this proactive approach needs to consider the balance between chances and risks associated with adopting AI systems. Considerations on how to quantify the investment in developing an AI-based CMS, and how to measure the return on such an investment have to be properly assessed.

3.4. Gaps in current literature

The literature review has provided valuable insights into how compliance management is addressed both from a theoretical perspective, and a practice focus. The various studies and articles that have been explored have set the scene for the elements considered in the data collection phase of the research. As an outcome of the literature review, two elements were initially considered highly necessary for putting an effective compliance program into practice: (1) a culture and infrastructure of compliance (human-based), and (2) a compliance IT system (computer-based). These elements have informed the data collection methods used by this study. The six categories identified in the debates within existing literature, are considered essential elements in achieving the enterprise-wide compliance management system in an organization, yet they must coexist in order to ensure the findings from this research reach the aim. Therefore, while this study agrees with previous research, it considers that the individual areas addressed contribute to the overall considerations towards how a CMS should work. Furthermore, an enterprise compliance management system requires a minimum understanding of its costs and benefits, and subsequently it requires an informed allocation of organizational resources between instituting the right corporate compliance values (first line of supervision) and charging managerial authority with oversight responsibility. If this research is to propose that the latter is supported more and more by AI, a lot more consideration has to be given to the risks involved with the use of AI systems. Russell et al. (2010) have a concluding subchapter, where they briefly discuss what the ethics and risks of developing AI are. Out of the six issues addressed, the loss of accountability is the biggest risk faced by an organization willing to deploy AI in its compliance management activities. It can be discussed that accountability and respective liability can be transferred from an individual level, to an organizational level, which then in turn leads to other form of compliance to the new rules. All in all, AI cannot be seen as the solution to make a system of managing compliance work smoothly overnight, as adopting AI requires more understanding of its real benefits versus the costs involved (e.g. costs of ideation, prototyping, development, testing, acceptance, production and subsequent maintenance). These are topics that go beyond the scope of this research and represent potential for future studies.

The current gap in literature on compliance management is three-folded:

- Current literature is primarily focused on the financial services sector (mainly banking) and pharmaceutical industry. This is primarily due to the fact that the past 10 plus years have seen a high response to the financial crisis of 2008, while the pharmaceutical industry is subject to extensive regulations.
- Compliance management is thematically addressed, yet the enterprise-wide view on compliance as an endeavour of the entire organization is missing.
- Artificial Intelligence-driven compliance management at the enterprise level is not addressed in the current body of literature.

Therefore, the second, third, fourth and fifth objectives of this research aim to close the gap of current research by capitalizing on the following points:

1. Use of retroductive argumentation for the development of critical realist grounded theory (theory that is grounded in the data, but theory-driven results through abduction and retroduction).
2. Study spanning one industry, but different organization types (different sub-industries).
3. Study covering compliance management systems across an organization, at all three lines of defence.
4. Multiple case study research method.
5. The use of Artificial Intelligence applications for the management of compliance, within each of the three lines of defence.

4. Research methodology

The ontology and epistemology of this research follow a commonly used approach in social science research, that of critical realism. The latter functions as a general methodological framework for research, not being associated with a particular set of methods (Fletcher, 2017). With this philosophical position, the ability to understand and ultimately determine conceptual guidelines of a compliance management system in organizations, is supported by the fact that humans stratify reality (Benton & Craib, 2011). First the nature of reality is determined (the common human perception of ontology) in the form of mechanisms, powers, tendencies found in reality. This is where the regulatory environment of an organization represents the mechanisms and powers driving the need for compliance. Secondly the knowledge of this reality is applied from the researcher's point of view, as the actual sequence of events is being discovered. Based on these discoveries (data collection) the empirical dimension of these events (epistemology) is pursued to be understood (data analysis). When trends in observed and captured events become obvious (they find themselves again and again in the collected data), these trends lead to the understanding of the reality being studied.

The thesis takes a critical realist approach, rather than a social constructivism one, because the research looks at an objective reality that exists independently of individual perception, while recognizing the role that individual subjective interpretation plays in defining reality (Taylor, 2018). Since social constructivism focuses on the things that are created through the process of social interaction (Taylor, 2018), the thesis could not take this approach as the nature of a system of compliance management in organizations is not driven only by social interactions, but driven independently by forces residing both outside and inside the organization.

4.1. Research philosophy

There are numerous examples of management papers that have employed critical realism as a research philosophy. This paper addresses the topic of compliance management systems, within the management sphere of business studies. In conducting the research, the axiological position is driven by the researcher's interest in lean and efficient use of resources within organizations and avoidance of work duplication and bureaucratic exercises that are often encountered when addressing compliance topics. Hence, the researcher takes a managerial axiological position.

The research subject area exists independently from our knowledge and beliefs about it, while current beliefs are open to further refinement based on on-going work such as this research

(Benton & Craib, 2011). This helps to position the research in the critical realist epistemology. Belfrage & Hauf (2017) describe critical realism as seeking to uncover mechanisms that generate, or cause phenomena that is observable. A system of applying compliance within an organization is highly refined by the beliefs of social entities (stakeholders within the organization), and hence these entities function together to generate the phenomena of a compliance system. To give an example, a company potentially decides how to arrange its compliance function during the meetings of its boards of directors and management. These boards are formed of individuals who bring their own beliefs and values to the table, and that will ultimately affect the way compliance management is addressed. The consequences of applying their values are the influences on procedures put in practice, depending what they believe the procedures are for. This can be argued to be a situation where causal powers determine the outcome of the compliance system, since the adoption of such a system is caused by the values of the individuals mentioned above.

4.2. Research strategy

This research is done using a qualitative method, of case study research. There are many reasons why case study research is suitable to the subject of study here, some of which are (Yin, 1994): the research focuses on a current issue that affects companies globally (management of compliance systems); the research is conducted in the real-life context of various organisations. Case study research is appropriate in the critical realism philosophy as it involves explanation derived from multiple instances of similar phenomena (Bray, 2015). Furthermore, guided by Yin (1994), the research uses multiple cases where the same phenomenon is expected to be found within the context of these cases (similar results, or contrasting results for predictable reasons). The expectation is based on the fact that the case studies belong to a population of large organizations, operating in complex environments, and therefore are expected to be subject to a high degree of regulations.

In order to generalize to a certain degree to new cases (Yin, 1994), a theoretical framework (based on a coding process, such as deductive codes used by Fletcher (2017)) is developed to support the entire research. Simultaneously, according to Eisenhardt (1989) the use of multiple cases allows the researcher to think in a creative way and generate theory with less bias than for example from axiomatic deduction. Eisenhardt (1989) also mentions that theory that results from multiple case study research can be tested with constructs that are readily measurable, since these constructs have already been measured during the process of building theory.

The chosen case studies are instrumental and not intrinsic, they support the process of answering the research questions, and do not represent the object of study (Stake, 1995). At the same time, the case studies are treated in an exploratory manner, where insight into the structure of the compliance programmes of the selected cases helps develop a framework, model or theory. The case study design is embedded and includes multiple units of analysis. Criteria for interpreting the findings derive from the coding process within the data collection phase and are based on resulting propositions. Findings are then represented by themes to which these propositions can be allocated. The case study organizations belong to one industry, namely air transport, although each exhibiting a different core business and operations model. These organizations have provided enough data and context to make it feasible to not expand beyond to other industries.

The design is based, as already specified, on multiple case studies because findings are replicated across cases (Yin, 1994). Eisenhardt (1989) gives an example of selection of multiple cases for research (large British corporations in four market sectors) and notes how this selection has allowed researchers to control environmental variation in order to focus on the constrained variation due to the different sizes of the firms involved. Similar to Eisenhardt's (1989) study example, this research chooses cases from a defined number of market sectors, although the same overarching industry. The intention is for the conceptual guidelines within the chosen cases to replicate or extend the theory emerging from the research (Eisenhardt, 1989). The choice of the case study organisations for this research represents a combination of theoretical sampling and convenience and network sampling techniques. Through theoretical sampling, the population of organizations was reduced to only large organizations (with more than 250 employees), operating in an international environment, expected to deal with complex compliance environments and at the same time to already invest in automation and AI to some degree. Based on the researcher's personal network (convenience sampling), first contact was established, followed by the non-probabilistic network sampling technique, during which the organizations selected have agreed to participate in the research, considering the request has arrived though the professional network. When examining the suitability of the market sectors, it became clear that having three organizations as case studies from the aviation industry could limit the research. Yet, these three organizations are active in different market sectors when analysed purely based on the scope of their business. Therefore, the case study organizations accepting to participate in this research have been judged to be appropriate in order to satisfy the aim and objectives of this study.

4.3. Research approach

Research is conducted using an abductive approach as the circumstances of the compliance functions within organisations are used to generate testable conclusions about the recommended conceptual guidelines. Using the abductive approach, collected data is used to identify themes and patterns (open coding process) and create conceptual guidelines for compliance management systems within organisations. The abductive approach is a type of logic used by critical realists to generate explanations (Edwards et al. (2014) as cited by Bray (2015)); hence the position as a critical realist in this research is accentuated. Furthermore, retroductive grounded theory is used to apply theory to the data to suggest generative influences on compliance systems as well as organisations' context specific causal powers that determine firms to adopt formal compliance programmes. To structure the research process, Edwards et al.'s (2014) chapter on critical realism and grounded theory is used. Within Table 2, the content of the details and assumptions from Edwards et al.'s (2014) table is replaced with content applicable to this study (in some cases, the assumptions made by Edwards et al. (2014) are kept as is).

Table 2. The structure of the research process (adapted from Edwards et al. (2014))

Theme	**Sub-theme**	**Assumptions**
1. Subject matter	Compliance systems within organisations	Built using positivist approach, shaped by values and culture (this is a strong assumption verified during the research).
2. Ontology	Critical realism	Stratified reality levels – causal powers operating in the three levels: real, actual, and empirical.
3. Methodology	Retroductive grounded theory	Applying theory to the data to illuminate and/or suggest generative causal powers as well as context-specific causal powers.
4. Data collection	Exploring lived experience through interviews	Designed to assist respondents to elicit recollections. Assumption of limited awareness of causal powers in the actual and real stratified levels.
5. Data analysis	Retroduction through coding	Applying theory to the data to illuminate and/or suggest generative causal powers as well as context-specific causal powers.
6. Theory development	Retroductive explanation	Explanation provided of generative causal powers that explain compliance systems. Contrastive explanations of causal configurations between contexts.

Using the abductive approach described above, the research design is based on a qualitative method (semi-structured interviews) in a single phase of data collection and analysis. The single phase allows for results to be interpreted simultaneously, based on retroductive grounded theory data analysis. Fletcher's (2017) empirical data collection method of observing events using two types of data is explored within this research. The extensive type of data referring to trend data (or statistical data) from publicly available data sources (online sources) is not used within this research. The second type, the intensive data, is the actual collected data (through interviews and documentation provided by the interview partners). According to Fletcher (2017), these data lead to the ability to code the information and identify demi-regularities, to support its analysis. Demi-regularities are tendencies (not laws) that can be seen in rough trends or broken patterns in empirical data (Fletcher, 2017). Sources of data are therefore two-folded: interviews (semi-structured), documents and archival records (these data sources provide a basis for confirming the 'real' world of what is to be studied, this being the first level of the reality stratification introduced by Roy Bhaskar). The interview questionnaire used for the data collection of this research can be found in Appendix E.

Context is very important in data collection, which is supported by the critical realist-informed grounded theory, as opposed to simple grounded theory that prefers context-free objectivity (Edwards et al., 2014). The impact of the critical realist-informed grounded theory on data collection methods can be looked at based on Bhaskar's (1978) arguments on the need to 'test' theories in reality, against a pragmatic common referent. In essence, it is attempted to demonstrate that the theory presented fits the lived experience of compliance systems. This demonstration shows how the conceptual guidelines for compliance management systems are now described through the data collected, emphasizing the familiar part of it (Fleetwood & Ackroyd, 2004). In collecting data, grounded theory guides one to move in a systematic way by collecting data based on categories related to compliance systems, linking the categories, and then move to selection of relevant data to form a homogeneous story, which eventually explains the compliance system phenomenon (Edwards et al., 2014).

4.4. Results and findings approach

The "Results and findings" chapter is practically split in three parts: (1) research propositions and connections; (2) results from data collection and analysis; (3) thematic structuring of propositions. In a nutshell, the research propositions represent the results of the research, while the thematic structuring represents the findings of the research.

The analysis of the collected data has been on one hand thematically driven by the coding process. This process consisted of the following steps: coding led to propositions (data source being the interview data); different documentation data sources allowed a matrix classification of the data in light of the propositions developed initially (data source being the documentation data); the propositions and the matrix classification represent the results of the research. Propositions have led to the creation of themes (data source being the interview and documentation data), these representing the findings of the research.

4.5. Discussion of the findings approach

From a theoretical point of view, the discussion part of the research findings is two-folded: (1) thematically addressed; (2) discussed at the three line of defence level (within each theme).

This approach allows the discussion to be contextually grounded (themes) in the collected data, and also to be related to the relevant theory that resulted from the reviewed literature (three lines of defence as a framework of analysis for enterprise-wide topics in organizations).

From a practical point of view, the discussion chapter is split in five parts: (1) theoretical framework, (2) discussion based on theoretical background, (3) discussion based on thematic results and recent theory, (4) recommendations, (5) limitations and recommendations for future research.

4.6. Impact of philosophical approach on results and conclusion

Following the completion of the research, recommendations to organizations are made, on conceptual guidelines for compliance management systems driven by AI. Therefore, the entire research is both practical and systems-oriented, results being applicable to business. The analysis of data using critical realist-informed grounded theory supports this approach and ensures that the importance of theory in the research development is not played down. Through using grounded theory, which was founded with the intention of creating new theory that is sourced within the underlying data, and not linked to existing theory (Fletcher, 2017), this research provides value to firms' facts concerning the compliance systems driven by AI. It is believed that by combining abductive data collection methods, and then retroductive argumentation with critical realist-informed grounded theory for data analysis, the research can generate testable conclusions on conceptual guidelines for AI-driven compliance management systems.

It is the aim of this research, to provide a deeper understanding of a phenomenon through the investigation of the strategic set-up of compliance management systems in large organizations and the degree to which they are supported by AI. The resulting guidelines for deploying an enterprise-wide compliance management system enabled by AI, are depicted as conceptual, and in this way are not intended to be generalizable, rather provide the concept based on which the practice can built upon within their own context. Here another explanation on why critical realism approach is used – the context of the studies cases is highly important, and the research obviously leads to conceptual results only, and not generalizable ones.

4.7. Originality

This research is an original piece of work, since the topic of enterprise-wide compliance management system and the understanding how AI can support this system, has not been researched to date. At the same time, the results of the research prove original, through the fact that they look at the overall picture of an organization and are not function/department specific. While a lot of discussion is ongoing on how digitalization and automation are affecting compliance management, no study has looked at the topic from the angle of this research, understanding how compliance systems can be at their own end enabled by automation and AI, or at how people, the infrastructure and the processes that compose a business, can benefit from (be augmented by) automation and AI to address the emergence of, and adherence to internal and external regulations and standards.

4.8. Limitations of the current study

The extent to which a case could be studied as whole is a limitation of this study, primarily as a consequence of no access to interview partners. The snowball sampling technique used, has been effective in gaining acceptance of participation of the organizations and to the limited number of interview partners. Yet, the technique has limited the ability of the researcher to reach out to other interview partners, who could have offered the confirmation or further depth to the collected data. Furthermore, since the research is conducted using an abductive approach, abductive reasoning is expected where observations are incomplete, and result in drawing the best possible conclusion, which establish causal powers encountered within the first (real) and third (empirical) levels of stratified reality. A study that would make sufficient specific observations and would encounter causal powers within the second level of stratified reality, would have to be conducted through ethnography, allowing for complete observations of the studied phenomena (the system of compliance management within the organization), and for the chance to be part of the intangible, lived aspects of a system of compliance management. Such a research would likely lead to specific observations and therefore would be capable of drawing general conclusions.

4.9. Limitations of other research philosophies

Employing other research philosophies to conduct this research would not be ideal to reach the findings and respective research results and conclusions. Here are the limitations seen in other approaches, and how these approaches would not be suitable to this subject research area. The research 'onion' introduced by Saunders, Lewis, & Thornhill (2009) is a good visualization of the available philosophies based on the epistemology spread: positivism, realism, interpretivism and pragmatism. Since the chosen research philosophy for this research is critical realism, this falls on the path between realism and interpretivism. On the ontological spectrum, the objectivist position is regarded as one that would tell the researcher what to be interested in, something that can be empirically proved (interested in the real world of companies and what can be demonstrated through hard facts) (Benton & Craib, 2011). This strict version of empiricism has difficulties in accepting that there is a more in-depth explanation of the world, the stratified version of it, which can be explained though a subjectivist ontology (Benton & Craib, 2011). Given the three levels of reality used to conduct the research together with the retroductive argumentation for analyzing the data, it is clear that an objectivist approach would hinder the understanding of context and causal powers in shaping compliance systems within organizations. Moving forward to the acceptable knowledge defined by epistemology (mentioned above), it is argued that anything other than critical realism has limitations in allowing context (values, company culture, history, interactions) within organizations to shape a role in providing conceptual guidelines for compliance systems in conjunction with actual objects of study (non-human systems). Positivism condemns one to a value-free research, where anything other than what can be hypothesized and subsequently tested is unacceptable (Saunders et al., 2009). On the other end, interpretivism can bias the researcher quite strongly, since it implies empathy with the research phenomenon (Saunders et al., 2009). This can lead during the data collection period, to potentially overlooking certain factual aspects that can represent excellent data to meeting the research objectives. In the sphere of values, an axiology where values would be missing would lead to first of all ignoring the researcher's own values, the understanding and knowledge of organizational dynamics, and secondly ignoring the values of the social actors that form an integral part of an organization's systems. Furthermore, the results of this research are to be applied in practice (it is a practitioner's research), the very practice that has provided the values mentioned above. Taking a positivist stance would rob the researcher from the core beliefs that have been the drivers behind this research.

5. Data collection and analysis

The data collection has been conducted by exploring lived experiences through interviews with representatives from the three case study organizations sampled. The interview structure and questions were designed to assist respondents to elicit recollections. The assumption has been of limited awareness of causal powers in the actual and real stratified levels and, therefore, documentation was collected as well, to form part of the data analysis phase.

5.1. Organizational context of case studies

The three case study organizations selected as instrumental to the achievement of the aim and objectives of this research, pose both similarities (overarching aviation industry) and differences (core businesses as association, airline, airport). Below is an introduction to the organizational context of each of these case studies.

5.1.1. Introduction to the case studies – case 1

The organization that represents case number 1 of the research is an association active in the air transport industry, where it represents and serves the airline industry. Through its work, the organization is developing global commercial standards meant at simplifying processes and increasing passenger convenience while reducing costs and improving efficiency (IATA, n.d.-b). Additionally, professional support is provided to all industry stakeholders with a wide range of products and expert services (IATA, 2020).

Data collected from case 1 has been in two forms:

- Interviews:
  - Head of Business Intelligence (BI) projects and industry engagement
  - Information Technology Services (ITS) director and Chief Information Officer
- Documentation:
  - Code of ethics and business conduct

Other analyzed data was procured from the following sources:

- Corporate website pages
- Company registrar

One of the cornerstones of the organization's offerings is the financial services provided to airlines, airports, air navigation service providers, travel professionals, catering, maintenance and repair, ground handlers, civil aviation authorities. In a nutshell, the organization handles the settlement between parties, and that means it handles sums in the area of e.g. in 2017 $433.3 billion (IATA, n.d.-a). The organization acts much like a bank to its clients. This makes it clearly one of the riskiest areas of business for the association. The financial services available consist of (not restricted to): settlement, e-invoicing, payment, card services, and other solutions. The category “other solutions” refers to flexible and reliable worldwide electronic data exchange and data distribution service available to the industry (IATA, n.d.-a).

The above presented business services make the organization’s key risk areas obvious: data related to financial services and financial settlement as well as other data management solutions (exchange, distribution). In the case study analysis, it shall be seen how due to this fact, there is a strong emphasis within the organization’s strategy on relying on automation/AI for information security and data management.

5.1.2. Introduction to the case studies – case 2

The organization that represents case number 2 of the research is a commercial firm active in the air transport industry, where it provides air transport services of both passengers and cargo. On one hand the organization belongs to a wider air transport group, which owns several air transport companies (with similar services to those of the case study). On the other hand, the organization is a group by itself, owning several subsidiaries. To understand what we refer to, we will call the former the “parent”, and the latter the “subsidiary”.

Data collected from case 2 has been in two forms:

- Interviews:
    - Compliance counsel
    - Head of Information Technology (IT) applications operation management
- Documentation:
    - Code of business conduct (subsidiry)
    - Code of conduct (parent)
    - Compliance committee meeting minutes (1 sample)
    - Legal structure chart

Other analyzed data was procured from the following sources:

- Corporate website pages
- Company registrar

The purpose of the company is the operation of an airline for the transportation of passengers, cargo and mail at domestically and internationally (Basel-Stadt, 2020).

The three key quantitative risk areas of the organization (as identified by the parent) are fuel price movements, cyber and IT risks, breaches of compliance regulation, while the three qualitative risk areas of the organization are flight operations risks, pandemic diseases, human resources (Deutsche Lufthansa, 2019).

5.1.3. Introduction to the case studies – case 3

The organization that represents case number 3 of the research is a commercial firm active in the air transport industry, where it provides scheduled passenger and cargo air transport services on the ground, together with other business support service activities (commercial services).

Data collected from case 3 has been in two forms:

- Interviews:
  - Deputy General Counsel (Legal department, part of the Sustainability, Reputation and Risk division)
  - Head of Innovation and Intelligent Automation (IT Innovation & Automation)
- Documentation:
  - Code of business conduct

Other analyzed data was procured from the following sources:

- Corporate website pages
- Company registrar

The purpose of the company is dealing with aviation business, advertising, ground handling, cargo, flights, parking, business lounge, restaurants, and shops.

Key risks to which the organization is exposed, are: halt of one of the key operational systems (e.g. baggage system, landing system, flight operations), inoperability of air traffic control (no aircraft coming in or departing), safety and security (landside and airside).

5.2. Ensuring right sample size and high quality

The sampling technique employed for the selection of case studies has been a non-probability one, namely the volunteer technique know as snowball or network. Initially a number of candidate organizations have been listed, and then based on the personal network of the researcher, key contacts have received the request of participation in this study (see Appendix D). Based on the principle of snowballing, the request has reached the right people in respective organizations, and these people have eventually accepted to be interviewed in the data collection phase. The subjective element of this sampling technique is represented by the fact that the researcher has reached to those known people in the professional network. The snowballing process that followed can be considered targeted, as key roles of people in the organization were sought after, and not random employees along the way. Of course, reaching those specific people came to the researcher through snowballing, as initial contacts have passed on the request within their organizations. Out of all the organizations asked to participate, the positive answers came from the same overarching industry, aviation, which means that the analysis offers an industry perspective and focus. The quality of the sample and the right size have been ensured by requesting in the first place to interview two or three people holding one of the following roles (any variation to these titles being accepted):

- Chief Compliance Officer / Compliance Officer
- Chief Digital Officer / Head of Digital / Digital Manager
- Chief Financial Officer / Head of Finance Operations / Finance Operations Manager
- Head of Digital Innovation / Digital Innovation Manager
- General Counsel / Head of Legal Affairs / Senior Legal Counsel
- Chief Technology Officer / Head of IT

The interview partners from the three case study organizations did not have one to one corresponding roles. This is the case because of different divisions of labour and it is acceptable in the context of this research, since the study is not meant to compare and contrast data based on function-specific particularities. The understanding of various perspectives from people holding a variety of roles, and belonging to organizations with different business operations, enables the identification of demi-regularities and paves the way for a wider spectrum of analysis, brining up more areas of potential future research.

Getting more than two or three participants out of the list of roles listed above was not feasible, due to time constraints. The two interviews conducted with each organization have provided sufficient data to consider reaching data saturation, as themes were recurring with the second interview already. Other criteria included length of each interview (approximately 1.5 hours) and conducting the interview in person. Additionally, participants have been informed in advance that supporting documentation would be requested (within the limits of data sharing and non-disclosure permissions). Each participant ahead of any data collection has signed a consent form, in line with the approval by the ethics committee of the home university.

5.3. Data coding and reporting

The collected data, classified as intensive data type by Fletcher (Fletcher, 2017), led to the ability to code the information within and identify demi-regularities, which are tendencies that can be seen in rough trends within the empirical data. Hence the coding has been applied to the interview data, and not to the documentation data. The latter has been used within the retroductive argumentation and thematic analysis/structuring phases, and later in the "Discussion" chapter, by showing how the two sources speak to each other, reinforce results and confirm the research propositions and themes. The coding documentation can be found in Appendix A. The categories of the coding are a direct representation of the categories used in the interview questionnaire (see Appendix E), while the questions types represent the key topic of each question within the interview questionnaire.

The result of the data coding process of interview data is a relational database design, where codes grouped by propositions allow reporting back the data (Atkinson, 2002). The data related to documentation analysis is analysed as a matrix, split on types of documents, and then linked to either the outcome propositions of the research or to the resulting themes. The report of the documentation data is available as a matrix design (see Appendix F).

5.4. Analysis method

The way the data collected through case study research has been analysed, is based on the philosophy of critical realism-informed grounded theory. By combining thematic analysis and retroductive argumentation, the phenomena observed within the case study organizations bring light to the causal powers that can explain these studied phenomena, and support the development of concepts and theories. The latter are nothing else then the outcome of this research: conceptual guidelines for an AI-driven enterprise compliance management system.

5.4.1. Data analysis based on critical realist-informed grounded theory

Edwards, O'Mahoney, & Vincent (2014) provide a practical guide to studying organizations using critical realism. One of the chapters of their guidebook addresses critical realist-informed grounded theory. They showcase how by using this approach, enough details are gathered to be able to shed light on the aspects that raise the question of “how” within case study research. Furthermore, they draw upon retroductive argument (Bhaskar, 1986), identifying generative causal powers that shape processes and practices with a given context, and then demonstrate how these generative causal powers coexist with local emergent causal powers (Edwards et al., 2014). Oliver (2011) describes retroduction as being abduction with a specific question attached, and therefore seeks explanations within the mechanisms that generate the phenomenon. To accentuate this, Oliver (2011) says that critical realist grounded theory ultimately pursues emancipatory, rather than simply descriptive goals. By saying “emancipatory”, it is referred to those goals that give social and political freedom. In the context of my own study, this approach stands out to be a good fit. This is because I expect the general requirements that drive organisations to build a compliance system to be brought into the internal environment and subsequently to be contingent upon local, internal causal powers (such as the general attitude towards systems and management) and to be highly dependent on local culture, hence the freedom to be shaped by the organization’s own culture.

Looking at the opponents of using grounded theory within a critical realist research, Fletcher's (2017) explanation that grounded theory is a data-driven, while critical realism is a theory-driven analytical process, is fair but not fully justifying the non-suitability of this analytical method. Fletcher (2017) mentions that grounded theory is grounded in the data, avoiding an active engagement with existing theory during the process of data analysis, which overlooks concepts drawn from other sources. As a matter of fact, grounded theory provides the freedom to the researcher to develop original theory, which is factual (due to it being based on facts resulting from the collected data). This theory can be subsequently tested, avoiding the bias of existing theory. On the other hand, agreement to Fletcher's (2017) view exists, stating that data processing is a very important step in critical realist research, representing the beginning of abduction and retroduction. The processing of data leads to identification of tendencies in rough trends or broken patterns within the collected data (Fletcher, 2017), supporting the coding of the qualitative data.

According to Edwards et al. (2014), ‘retroductive argumentation is most relevant to the development of critical realist grounded theory when there is the assumption of causal powers within a stratified reality’. This stratification of reality has been introduced by Roy Bhaskar and implies three levels (Benton & Craib, 2011):

1. The ‘real’ world of what is to be studied and discovered (mechanisms, powers, tendencies).

2. The ‘actual’ sequence of events, which occur outside the laboratory, but rather in lived conjunctures.
3. The ‘empirical’ dimension of observed events, which are a subset of the second level of ‘actual’ events.

For this research, the stratification of reality is a logical approach to studying the phenomenon of a compliance system in organizations. The ‘real’ world level is represented by what a compliance system should be according to handbooks and management research, as well as to regulatory oversight agencies. The second level of ‘actual’ events represents what the company and its employees actually do to live and maintain the compliance system; this context is nevertheless not discoverable through this research. The third level, the ‘empirical’ one is being discovered through data collection and analysis within this research.

The analysis of the collected data has been on one hand thematically driven by the coding process. The process consisted of the following steps: coding led to propositions (data source being the interview data); different documentation data sources allowed a matrix classification of the data in light of the propositions developed initially (data source being the documentation data); the propositions and the matrix classification represent the results of the research. Propositions have led to the creation of themes (data source being the interview and documentation data), these representing the findings of the research.

5.4.2. Thematic analysis

The theory that results from the multiple case study research can be tested with constructs that have been measured during the process of building the theory (Eisenhardt, 1989), respectively the result of the literature review phase represented by the split on categories and propositions. These categories were used in the data collection phase, and have led to propositions. Ultimately, these propositions were analysed using retroductive argumentation and have led to the thematic split that can be found in the “Results and findings” chapter.

5.4.3. Retroductive argumentation

The analysis method employed has been retroductive argumentation, which applied to the themes and literature review categories, has led to recommendations. These recommendations represent the contribution to theory and practice and form part of the chapter 9 of this research. Furthermore, in analysing data, Bhaskar’s three out of four stages of retroductive argumentation within the context of the case study research are used (similar to Edwards et al. (2014)):

- Description of a phenomenon – the perspective of the lived compliance system within organizations.
- Description of causal powers that produce or are a condition for the phenomenon of existing compliance systems (including individual values, corporate culture).
- Development of theories and concepts (conceptual framework based on open coding) to explain how causal powers shape events within the compliance system of the organization.

The fourth stage, testing theories in reality based on actual experiences within organizations, is not employed as it goes beyond the scope of this research.

6. Empirical results

The data collection and analysis culminated in the formation of final research propositions, which are outlined in this chapter as results of the study, together with the key findings. These findings are here only listed, and are further discussed in the next chapter in light of the literature review, the CMS framework (theory) resulting from it, as well as in light of new developments in the practice and in theory.

6.1. Research propositions and connections

Following the theory of critical realism research, the analysis of the data from the three case study organizations has been based on a coding process. This coding process represents the skeleton of this research, the theoretical framework allowing for future generalization to new cases (Yin, 1994). The categories of the coding (Appendix A) are a direct representation of the categories used in the interview questionnaire (see Appendix E) and expand into rationalized codes, leading to propositions. The common attributes of the data clustered under these propositions have blended into nine themes, outlined at first in sub-section "6.3. Thematic structuring of propositions", and further elaborated in chapter seven "Discussion". This thematic discussion, mixed with the theoretical background and the conclusion of this research, have led to the recommended conceptual guidelines (see chapter 9) of this research, fulfilling the ultimate aim. In order to conceptualize underlying patterns (Gibbs, 2013), which corresponds to the act of describing causal powers according to Edwards et al. (2014), the research propositions and their connections are explained within this section.

The initial literature review has split the debates into six categories (see "Debates in literature" in the "Literature review" chapter), which represented the basis on which the questionnaire (refer to Appendix E) used in the data collection phase of the research was designed. The questionnaire included four initial areas (categories) of exploration: (1) general/introductory topics, (2) technology in compliance management, (3) people and (4) other. When analysing the data, a number of propositions came to light, which could not be allocated to any of the initial areas of exploration. These were first clustered under the area (5) "new themes and codes". The new propositions have derived out of the coding during the data analysis phase based on the common reiteration, while the old propositions remained relevant once the data was collected. The propositions represent the results of this research in a raw format, and are to be found in the next sub-section of this chapter (6.2. Results from data collection and analysis).

Below are the details of the categories covered in the data collection phase:

1. General / introductory topics – this area focused on gaining an overall picture of the organizational setup, setup of the compliance function, responsibilities, strategy for solutions, maturity, enablers and barriers of AI technology adoption.
2. Technology in compliance management – this area investigated what technology is currently used by the compliance function, what AI applications/tools are used for compliance management in particular, how compliance by design is addressed, whether or not, and what predictive and prescriptive models are deployed towards risk and compliance management, as well as any other tools used by the three lines of defence.
3. People – the area related to people investigated the reporting structure of the compliance function, as well as the existence of dedicated compliance personnel per business line/department. At the same time, the focus here has been on finding out what tools/applications are used by dedicated compliance staff, and last but not least, uncover how training towards compliance topics is conducted.
4. Other – this area has packed together topics that support the second research objective, of analysing the setup and design of CMS within the case study organizations.
5. New themes and codes – born out of the data collection phase (interviews), this area is key towards achieving objective number five of the research, due to the fact that these themes reveal underlying patterns within the case studies. As such, the identified themes provide insight into the enterprise-wide requirements towards reaching a desired state of a compliance management system, which is ultimately enabled by AI. Three themes here reveal the importance of external stakeholders: relationship with regulator, global standards of standards coming from national authorities, collaboration with external parties. The other four themes (data management, cyber security, ethics, and IT infrastructure) reveal prerequisites or considerations that could either enable or disable the adoption, deployment and productive use of AI applications.

6.2. Results from data collection and analysis

Before moving into the key themes that represent the findings of the research, below are the results of this study, first from the interview data collection and analysis structured by the thirty-four propositions, and second from the documentation analysis. The common elements found in these results, drive the clustering of the common themes presented in "6.3. Thematic structuring of propositions". A full table of the research propositions can be found in Appendix A (categories, codes and definitions). It is important to make reference to Appendix A, in order to understand the overall common themes.

6.2.1. Results: interview data, analysis and propositions

The following thirty-four propositions have resulted from the interview data and its analysis. Each proposition presents the results as they have been coded per case study, hence case 1, case 2 and case 3 will appear to distinguish the provenance of the results.

1. Examples of automation or AI applications/tools that the organization currently has in production (operational) or finds itself in a trial-phase (regardless of the area/department/function):
   a. Case 1 is working on a data exchange platform, and already has many rule-based applications using data structured in a database; AI is limited to the IT department; using machine learning to detect/anticipate third party fraud; automated control for email verification tracing malicious code within email and attachments, rule-based user access.
   b. Case 2 has many automation/AI applications related to its core operations. These include: revenue management, flight planning, crew planning, flight operations/irregularity management, chatbots, voice assistants, passenger check-in automation, direct ticketing sales over Google (automated distribution systems); new collaboration with cloud provider for flight optimization projects.
   c. Case 3 also sees a number of applications focused on its core operations. These include: autonomous vehicle pods, automated baggage system, stand analytics and planning (using computer vision based machine learning), trials with robots (studying interaction between humans and robots), chatbots, analytics and visualization of operational data, passenger forecasts, airport environment simulation (using digital images to teach machine learning algorithms).

2. The general/overall strategy of the organization when it comes to automation/AI solutions:
    a. Case 1: outsourcing of AI skills (combination of in-house and third party), create a consistent ecosystem of data management practices, apply rule-based actions for everything that uses data, create internal capabilities, tap on its relevance to clients for data processing, ensure sufficient data is available, modernizing old processes and controls through automation.
    b. Case 2: high in-house development, ITIL-process oriented IT operations, avoidance of cost-intensive projects, service-oriented middleware products allows for cheaper and more flexible products (providers are generally limited in the industry), hiring of data scientists across departments, AI for irregularities management, landing operations improvement, adoption of cloud computing for optimization, larger IT development team available to the group, core focus is on the so-called “policy compliance tools”.
    c. Case 3 has a major back office transformation project, which will include certain levels of automation. Other projects include: known digital identity concept, big leaps for corporate functions with regards to technology advancement, aim for consistency of maturity across the board, learning from trial/prototype projects and implement elsewhere, designating a transformation team in charge of the innovation and automation programme, developing the new organization-wide management system, equipping colleagues with the right technology, augmented reality for engineers, more chatbots in the airport environment (for passengers), baggage system automation (a lot of data available), working together with partners towards fully automated terminals/stands (no human interaction), experimenting automated movement of bags/people/catering (any airside operations requiring humans).
3. The strategy of the organization when it comes to automation/AI solutions to support the management of compliance / activities of compliance management:
    a. Case 1 does not seem to have an AI strategy for compliance. It prioritizes compliance in everything it does, so it is an active subject across all projects/programmes. Plans exist to automate third party financial risk assessment and prediction of materialization of default. A lot of focus is put on the cyber security area and controls automation (security automation tools); it

   also considers how the compliance preoccupation will be tackled through the software development lifecycle.

   b. Case 2 does not seem to have an AI strategy for compliance. Compliance requirements in general are high and voluminous.
   c. Case 3 is working on an enterprise-wide management system, which is to be designed with the considerations around compliance. Departments allocate directors in charge of transformation for the development of this management system. The strategy is to bring consistency and reach a certain level of maturity across the enterprise (equivalent of a six or seven on a scale from one to ten).

4. The level of perceived maturity of the organization's automation/AI solutions:
   a. Case 1 considers not being very mature as an organization when it comes to AI. Maturity exists to meet certification requirements (from an IT perspective).
   b. Case 2 considers being at the beginning of adopting/implementing AI solutions especially in the legal/compliance unit, with other areas potentially being more advanced.
   c. Case 3 considers certain areas of the business to have a high maturity (equivalent of an eight on a scale from one to ten), with others having a low maturity (scoring one or two on the same scale).
5. The factors/topics that are enabling the organization to adopt automation/AI technology across the board:
   a. Case 1 mentions the following enablers: strong data management practice, sufficient and right data, good senior management support in creating internal capabilities, reduction of complexity and allowing personnel to focus on real business activities, good results driving demand for more AI solutions.
   b. Case 2 mentions the following enablers: easiness to comply, helping managers to take decisions by themselves, legal requirements make it imperative to adopt AI solutions, senior management support, cost savings, improvements for the customer, size of the company group (economies of scale).
   c. Case 3 mentions the following enablers: good results showing benefits and hence driving demand for more AI solutions, buy-in from senior managers for such solutions, increased customer experience, increased employee well-being, reduction in FTEs, adaptable AI with data interpretation capacity, breaking out the linear relationship between OPEX and CAPEX, network availability and

competitive power of AI, safety and security drive compliance activities, cross-industry collaboration and sharing of lessons learned, wider acceptance of certain technologies, change in easiness and costs of implementation.

6. The factors/topics that are stopping/blocking the organization to adopt automation/AI technology across the board:
    a. Case 1 mentions the following barriers: weak or inexistent data management practice.
    b. Case 2 mentions the following barriers: larger size of the organization's parent, amount of people involved in alignment and decision-making, matrix organization, procurement function, heterogeneous application landscape, involved costs, monopolistic distribution channels.
    c. Case 3 mentions the following barriers: resistance to change, involved costs, fear of ending up in the "arms" of computer programs or algorithms, false "high risk" perception, binding to a system without alternatives, making it comprehensive compliance showing merits and cost benefits, innovation is faced with the hurdles of compliance due to safety and security (e.g. permission restrictions for proof of concept projects / trials), liability topics for third parties, demonstrating return on assets or capitalizing investments, agreement on investments with other stakeholders or partners, obsolesce of technology by the time it gets approved and operational, high level of due diligence, high number of stakeholders increasing compliance requirements, compliance with regulation that is not adapted to the new needs.
7. The structure of the organization: departments, units, etc.:
    a. Case 1: representing member airlines across the globe, has regional vice presidents for Asia-Pacific, Africa & The Middle East, Europe, The Americas; on a functions level, it is split into airport, passenger, cargo & security, customer & business services, financial distribution & data services, member & external relations, safety & flight operations; in addition, functions for people and development, general counsel, corporate communications, corporate services and finance exist.
    b. Case 2: part of a group organization, matrix organization, process-oriented, own local structure with different business lines, some fifteen data scientists.
    c. Case 3: the organization has four tiers, namely operations, commercial, expansion, support staff (business assurance, legal, IT, finance, people

strategy). It is a regulated business and hence the commercial income is offset partly by the costs of running the operations, the surplus going to shareholders.

8. The structure of the compliance department/function (e.g. position within the organization, reporting lines etc.):
    a. Case 1: different layers of risk and compliance across the organization, dedicated compliance function, business areas are empowered with additional support from specialized units (compliance, legal, risk), risk management decisions lie with the business (accept, mitigate or transfer), risk champions designated within business areas, in some areas risk managers are appointed, some divisions have their own risk “department”; anti money laundering compliance, GDPR compliance, standards compliance (e.g. ISO 27001, SOC 2, PCI DSS), third party due diligence.
    b. Case 2: the compliance department covers four key areas (integrity, competition, embargo, capital markets); first line of defence is being trained; second line of defence compliance counsel responsible for the organization’s compliance and partly parent’s compliance topics and to inform other departments of what they should be compliant with (out of the areas in the jurisdiction of the compliance department); compliance counsel reviews and investigates cases; third line composes of two parent internal audit teams plus two local members of staff for the function and is responsible for monitoring of policies, procedures; centralized business process applications; local law drives customized guidelines; three compliance teams exist (services, processes, airline) where the processes team is responsible for developing new guideline or the adoption of guidelines (or applications).
    c. Case 3: sustainability reputation and risk function part of support staff tier (includes communication); business assurance team covers risk and audit, legal team covers data protection, business assurance and legal teams communicate to the rest of the business.
9. Information on the existence of a formally named "Compliance Management System (CMS)":
    a. Case 1: a CMS is in place, policies exist, training delivered to the users, process is set up, third line of defence (internal audit) has access to security tickets / monitoring to check compliance (adherence) to the cyber security programme; auditors are trained (on SOC 2 and PCI DSS).

b. Case 2: CMS has four elements (similar to the parent CMS) – integrity (anti-corruption, anti-bribery), competition, embargo, capital markets. All group companies follow one CMS as the parent company is listed in Germany.

c. Case 3: the organization does not have a CMS, as compliance responsibility is spread across various teams within the support staff tier; the aim is to create a safe system where increased standards need to be lived, people need to be comfortable with the outcome of their work all while a minimum level of work is unlikely to create the safe, constant conditions required for sustainable compliance management.

10. The responsibilities existing within the CMS:

    a. Case 1: CIO responsible for ISO 27001, SOC 2, PCI DSS compliance and reports to cyber security steering committee reporting to risk committee, part of audit committee, which is part of the board; anti money laundering compliance responsibility lies with the compliance department; within the business lines an account manager from the support units makes recommendations, while the responsibility resides with the business unit; ITS responsible for security awareness training and internal compliance breaches; SLAs defined with IT providers are monitored trough dashboards (e.g. days required to close incidents, vulnerabilities).

    b. Case 2: compliance counsel part of team airline and mainly responsible for compliance of the local firm and not the group (with exception of a few topics) – responsible for emerging topics; compliance managers report to the compliance counsel – responsible for adherence topics; compliance managers are only allocated to high risk business units; compliance such as accounting or finance is function specific and hence responsibility lies within the function (e.g. credit checks); compliance managers within the business units are responsible for the process they own (e.g. the process owner verifies requirements engineering compliance against compliance governance rules); within IT operations, compliance equals stable operations and avoiding too many changes (following the ITIL IT systems framework), with the team being trained and having the right skills.

    c. Case 3: a number of governance and compliance steps need to be taken in different areas (e.g. a standard form contract before entering into a contract), going through a gateway process; a RACI chart for the different tiers exists (e.g. commercial, expansion) to designate responsibilities of executive directors for the different business leads; most compliance comes from the project world, and small groups are involved looking at IT risk, cyber security; for data protection a GDPR data officer is involved in every trial; four people within the legal team deal with data protection issues, and they liaise with data protection champions within the business who hold accountability in their areas who make sure what they do is compliant with data protection regulations; the innovation team has to go around certain formal compliance processes, by using acceptable means of compliance in order to progress, meaning doing a few more things manually.

11. The responsibilities split between internal and external compliance topics, existing within the CMS (or equivalent):
    a. Case 1: natural segregation between the two; involving the account manager triggers internal compliance, while the account manager is responsible for specialization in external compliance requirements.
    b. Case 2: laws will be implemented within the guidelines of the organization and the responsibility lies with the compliance department; security and governance department responsible for internal compliance of e.g. IT operations.
    c. Case 3: a lot of things are driven by the relationship with the regulator or stakeholder (hence responsibility can be assumed to be with the relationship owner).
12. The list of technology applications/tools/other that are used by the compliance function:
    a. Case 1: the results are limited to the compliance tasks and responsibilities of the interview partners, and include: anomaly detection in user access management; not known if risk managers use any specific tools; AI for some controls; enterprise risk management tool triggering action plans and monitoring done using the same tool.
    b. Case 2: third party cargo embargo compliance tool; intranet used for accessing compliance documentation; eLearning for competition and integrity compliance; compliance risk assessment tool

   c. Case 3: automatic vehicle pods transmitting data for analysis of compliance and self-improvement; in general the organization has some fairly residual systems.

13. The list of automation/AI applications/tools/other that are used by the compliance function:
    a. Case 1: rule-based engine to check financial credibility of users; Power BI (Office 365) reports as dashboards for cyber security, GDPR; AI for correlation for security investigations, threat intelligence platform; security compliance rules built into the cloud service provider.
    b. Case 2: event management tool using a decision tree; eLearning for integrity and competition compliance; third party cargo embargo compliance tool; policy compliance tools in the core operations such as flight planning, crew management (forecasting and managing irregularities).
    c. Case 3: operations systems compliance (e.g. baggage system, self-boarding, other airport infrastructure).
14. How is Compliance by Design addressed within the organization (e.g. to what level and how it is ensured that compliance is embedded in the applications deployed across the organization, from an early stage):
    a. Case 1: fixed framework (happy scenario, less favourable scenario, built-in algorithms to detect/monitor and put measures in place e.g. prescriptive and active decision making); CbD is considered a no-brainer and the aim is to minimize the overhead for compliance monitoring by automating within the design, designing applications from day one, thinking about sanctions and embargoes and compliance; data management, governance, architecture are key, as regulations can force the design of a system from day one, but also need to think ahead; design a deterministic system by eliminating medium-level compliance; strive for processes engineered to be redundant where humans are involved, avoiding the chance to tamper with results, taking the human factor out if not required; testing is extremely important and needs sufficient data, plan in using more digital twins projects; special circumstances exist where you need to provide exceptions to the designed system (e.g. local admin rights) and here a CbD is to have means of tracking and monitoring; compliance process became part of the business process, hence today controls are implemented as part of all the processes of the organization to ensure

compliance with the policies agreed upon; due to the fact that compliance has to be addressed during the design phase, the IT and legal departments have become more and more integrated in business processes, rather than being simple support functions to the business.

b. Case 2: CbD is driven by the business, business requirements are translated to new IT applications through a role known as "IT to business alignment" – a responsible project person ensures addressing both business and IT requirements; policy compliance tools are built in the spirit of CbD as they are rule-based; project processes are closely managed and driven by the business needs, having a formal governance of project architecture; the rule is to first search for standard applications and then for solutions with a standard process.
c. Case 3: within the legal team, the considerations around CbD are not a priority, as with the new ERP system the adaptation will happen by tapping into the system adopted by the rest of the organization; introducing a new system or tool means the participation of all stakeholders (e.g. all business assurance team); cognitive questioning and embedding common sense into applications is difficult and these are some of the key requirements of a legal department; CbD within policies and procedures should make it easy for users to be compliant; compliance by design needs a lot of testing, and therefore practice data is a key factor in AI applications to be designed as compliant as possible; cyber security CbD is one of the most important requirements to design compliant systems; pilot projects to address security that ought to be addressed in the design of a robot, tool, application.

15. Predictive models currently in use by the organization towards managing compliance tasks:
    a. Case 1: tools predicting default chances of users (third parties); other forecast tools.
    b. Case 2: media scouting due diligence for third parties, allocating scores and predicting viability; predicting flight and revenue irregularities; other forecast tools.
    c. Case 3: forecasting tools; Microsoft tools for operational data and insights.
16. Prescriptive models currently in use by the organization towards managing compliance tasks:

   a. Case 1: one small area using prescriptive analytics at the moment (describing what the next best action should be and taking that action).
   b. Case 2: prescriptive irregularities steering based on predicted flight and revenue irregularities.
   c. Case 3: prescriptive operations such as flight paths where humans are in control and rely on prescriptive information; other ground handling such as stand usage and turnaround data.

17. The list of technology applications/tools/other that are used at each of the three lines of defence levels to perform their daily work tasks/routines:
    a. Case 1: integrity of a particular process based on built-in rules e.g. user access withdrawal (second line of defence); security operations centre e.g. anomaly detection, reports and monitoring security training (second and third lines of defence).
    b. Case 2: cargo embargo compliance tool (first line of defence); third party due diligence / background checks tool (second line of defence); compliance risk assessment tool (third line of defence); reporting tools, incident tools for providers, providers portals (second line of defence).
    c. Case 3: the example of the legal department being rather manual, so the use of augmented intelligence is limited; operations relying on dashboard data (first line of defence).
18. Existence of dedicated person per department/line of business/team, in charge with performing compliance duties:
    a. Case 1: account managers from the second line are allocated to the different business units; risk champions and risk managers exist within business units / divisions.
    b. Case 2: compliance managers allocated to high risk business units; compliance function has different persons for the three areas (services, process, airline); within operations there are process owners, functional and disciplinary lines.
    c. Case 3: experts within each area feed the business assurance and legal teams with on-going requirements, issues etc.; e.g. data protection officer champions who take on the responsibility.
19. Reporting structure and responsibilities of people in charge with compliance duties:
    a. Case 1: account managers are the gateway people for the business units to connect to the compliance requirements; decision lies with the business unit,

compliance expertise within specialized area; AML is a compliance department task.

b. Case 2: compliance managers are responsible for compliance topics/questions/cases and reporting and they represent an extended arm within their units, of the compliance counsel; two reports per year to the parent company; compliance committee has four meetings per year for reports approval and decision-making; implementation status of the CMS is tracked in a tool by the compliance counsel; reporting SLA compliance within provider service meetings, governance boards and IT meetings; monthly meeting with IT management; group IT security governance compliance meetings; when reporting, information from different tools has to be manually collected from the different tools and aggregated based on the target group.

c. Case 3: the organization strives for a culture of reporting; it has many suppliers and system interfaces do not exist apart from the interface to key operations stakeholders (e.g. air traffic control); analogue monitoring and reporting; liaison of champions in different areas with the business assurance teams of experts; accountable people are within business areas; training-wise, business people are often the experts in their areas due to the nature of the industry collaboration and sharing of best practices.

20. Applications/digital tools that people in charge with compliance duties use to perform their tasks related to compliance management:

    a. Case 1: measures in place to detect in an automated way areas that require attention from a integrity perspective, which means you know something is highly inaccurate or not, and from a quality perspective if there's lack of accuracy in certain things (data is already structured in a database) – analyse the database and detect what's happening in there; international databases for entity checking;

    b. Case 2: event management tool, cargo embargo compliance; the compliance counsel works mainly analogue with the typical eLearning and other Microsoft Office package tools.

    c. Case 3: document management system, e-signing.

21. Way and type of training provided to the organization's employees with respect to compliance management or simply compliance topics:

   a. Case 1: business lines are empowered to make their own decisions, they are trained on compliance topics by their allocated account managers from the specialized second line of defence units; trainings also offered as e-learning, monitoring of completion rates and first-time right also done; auditors are trained on information security and respective standards (hence third line of defence training also ensured).
   b. Case 2: e-learning tool for compliance topics (part of the learning management system); in IT operations, ITIL operations processes followed and staff are fully trained to comply to this framework.
   c. Case 3: doing the right thing has to be intrinsic, hence the organization strives for on-going training towards compliance; formalized monthly catch-up meetings on data protection; new legislation and new policies rolled out in formal sessions by the legal team; in certain areas there is no documentation specifying the rules as the organization assumes inherently knowing the rules – advance information on compliance rules to third parties could be improved.

22. The way in which the organization is ensuring that silo compliance (compliance within e.g. departments, functions) is avoided and therefore compliance-related topics are aligned to the company policies, risk appetite, etc.:
    a. Case 1: involvement and alignment of account managers (legal, risk, corporate communication); policies are quite clear and represent the umbrella to everything; there is also a clear PMO methodology, documentation (alignment process for new implementations/projects: business case validation, review by IT department, security review, quality review of software development and project management, IT component compliance – architecture, information security, data privacy); bring data together with a data governance programme, ensure avoiding silos in cross data management.
    b. Case 2: the gap business-technical requirements is bridged by the IT process project manager, compliance manager is not involved in the implementation; steps in evaluation of new business tool needed involve multiple internal stakeholders (addressing compliance issues, availability as standard product, availability in the group, RfP overall evaluation, IT procurement considerations).
    c. Case 3: interfacing to third party systems is crucial (e.g. airport and air traffic control); dealing with residual, independently developed systems; culture of

avoiding silo compliance mind-set (requirements for those taking on director roles include them having worked in and experienced various areas of the organisation to avoid familiarity bias).

23. The way in which different departments/units interact with each other to align on company policies and other compliance-related topics:
    a. Case 1: four-eye principle applied; involving the account manager triggers internal compliance; intense involvement and collaboration between legal, IT and business units; project management methodology ensuring that any business team that wants to implement something has to go through a review by the IT department, an alignment process: security review, quality review in terms of software development and process development and project management. IT representatives involved in the validation of the business case, part of the signatories of the business case. For IT components, the CIO ensures that it will comply in terms of architecture, information security, and in terms of data privacy.
    b. Case 2: business and IT project managers work together in the requirements definition phase; steering committees for projects ensure the key people are involved (e.g. procurement, business, IT); IT to business relationship roles ensure mutual understanding of compliance requirements engineering (CbD, IT requirements etc.) as they have project leaders and IT business analysts; doing well with established governance on projects, waterfall agile approach; when business requires new tool, IT alignment cross-checks with available tools within the group and only then would start a formal RfP.
    c. Case 3: next to formal training sessions, ad-hoc access to the legal and business assurance teams is key in disseminating compliance-related know-how; there's a general fear on not being able to advise if the exchange is not done in direct contact with the person; designing policies and procedures is done in collaboration with the business and strives to make it easier for people to be compliant than non-compliant; within operations, collaboration with other stakeholders and other similar service providers and sharing of data to learn and improve together; innovation team has to use workarounds at times as compliance processes can be cumbersome, hence collaboration with the policy makers and the monitoring line (second and third lines of defence) is paramount.

24. Understanding the degree to which the organization's compliance system is monitoring-based (using professional auditors/third line of defence), a fact that represents very high costs for the organization:
    a. Case 1: the organisation only expresses the fact that monitoring and enforcing compliance are the areas with good opportunity for automation, while emergence of compliance rules and regulations is at the moment more human driven; audited on a regular basis by both external auditors and internal auditors; this will carry on as long as the organisation complies and as long as it has a continuous improvement process; from each audit, findings are entered into the enterprise risk management tool; all the audit activities result in findings that will trigger action plans, which are monitored; monitoring of exceptions to the policy through real-data dashboards (continuous monitoring); first line of defence has to complete the security awareness training, while the second line is responsible for completeness monitoring; periodic reviews of access control, rights and credential profiles; monitoring workstation compliance through dashboards; security operations centre responsible for anomaly detection, investigation, findings and prioritization of incident solving.
    b. Case 2: the organization has a lot of policies, procedures, training, and subsequently high levels of monitoring is required; economies of scale when it comes to costs of monitoring (third line of defence); audits output is very valuable, including penetration tests in the IT operations area.
    c. Case 3: monitoring is currently a mixture of more formalized structure and ad-hoc anecdotal components; monitoring of supplier data and SLA compliance done by taking data as provided by suppliers, and plugging it into the system; business assurance and legal teams identify areas of particular risk and create long-term forward-looking audit plan and a short-term forward-looking audit plan.
25. Type and way of auditing[1] and the degree to which audit activities support the compliance management activities of the organization:
    a. Case 1: audit happens systematically, business as usual; audited on a regular basis by both internal and external auditors; this will carry on as long as the

[1] The IIA's mission is to advocate, educate and provide standards, guidance and certifications for/to members working in internal audit, risk management, governance, internal control, information technology audit, education and security (refer to chapter 2.2. for details) (The Institute of Internal Auditors, 2020).

organisation complies and as long as it has a continuous improvement process; from each audit findings are entered into the enterprise risk management tool; all the audit activities result in findings that will trigger action plans, which are monitored; having to comply with external standards, which affect a large portion of the stakeholders (namely clients), the organisation lets itself audited every quarter by an external body, which stamps the adherence to the standards (e.g. PCI DSS); annual surveillance audit for ISO 27001; audit for GDPR is in the responsibility of the legal department, as GDPR compliance is assigned to the legal department; auditors are trained on information security, with audits happening every quarter.

b. Case 2: internal audit staff available locally, with a large organisation available at the group level; group-driven audits, many audits on compliance topics; the feeling is that the resources spent on audits / monitoring is well balanced, provides a good return/outcome; audits are valuable as they allocate priorities and allow to invest time to make things better/safer/easier, so resources spent on audits are considered to equal the benefits brought; anyone in the group can request an audit.

c. Case 3: in general there is the feeling that nobody wants to be audited, and that a formal compliance function would become a policeman; a mind-set change is required for people to aspire to do the right thing, desire audits with the aim for the audit results to help improve; the audit team identifies area of particular interest and will form a short and a long-term looking audit plan; flexibility exists in standard audit planning, to prioritize high risk areas and move audits in the system; audits reveal areas of non-compliance by third parties.

26. Type of resources consumed by the organization to run a CMS in order to break-even on the equation “resources = requirements”:

    a. Case 1: resources for compliance adherence (including monitoring) considered to be in a sweet spot regarding the amount of resources consumed for compliance activities; regular KPI reporting on budget spent on information security, using a benchmark; the culture of the company drives the need and allocation of resources; lack of resources is marked as a risk in the risk management system, likely not to be accepted by the risk committee as the culture is to not accept risks, but to always mitigate risks.

   b. Case 2: monitoring through audits is considered very important, with many audits being organized; audit outputs are very valuable to teams such as IT operations (allows for learning and improving); not known how much it is being spent, benefits are quantified in the satisfaction of having valuable outputs.
   c. Case 3: the new management system is desired to be more efficient in predicting things and sparing people from running compliance checks; the new system is built based on business cases, hence budgets and costs are calculated based on the principle of positive net cost to the organization.

27. Knowledge on the costs incurred by the organization to run a CMS (covering all the three lines of defence):
    a. Case 1: perception is of balanced resource allocation; results speak for having the right balance between internal resources and frequency of compliance work.
    b. Case 2: always trying to mitigate the risk of business discontinuity, in some cases, it has been decided to stop some businesses, because the risk was bigger than the benefit; if resources are not available, they will be marked as high risk to the organization, and the spent prioritization will be redirected towards compliance enforcing and checking (e.g. from the IT department).
    c. Case 3: the organization culture is positive, with people absorbing compliance in their roles; no further costs knowledge/information available.
28. The influence and involvement of regulators within the activities and decisions related to the management of compliance has a direct correlation to the overall CMS of an organization:
    a. Case 1: industry standards drive compliance activities and prioritization (e.g. PCI DSS); aim is to expand cyber security standards through the International Civil Aviation Organization (ICAO); pushing a global framework to be used across the industry within several areas.
    b. Case 2: *no comments.*
    c. Case 3: relationships with regulator affect both the organization and its service providers; decisions are often driven by the relationship with the regulators; important to work off similar systems, collaboration on procurement and requirements gathering, definition etc., ensure good setup and compliance on both sides; situation of permissive regulators, regulation is slow to adapt to

technology advancements, discrepancy between regulating authorities/bodies between different countries: e.g. Hong Kong and UK; important to start working with regulatory bodies to create industry standards; focus on developing standards as you go along; adaptation of existing frameworks: e.g. standard vehicle plus autonomous vehicle requirements; standards developed in collaboration with other service providers and the regulator (e.g. baggage custody considerations).

29. The influence of global standards or national standards on the compliance management system and the policies an organization adopts and implements within its CMS:
    a. Case 1: reverse is applicable here – organisation working on pushing global standards to the wider industry and to other countries; aim is to expand cyber security standards through the International Civil Aviation Organization (ICAO); pushing a global framework to be used across the industry within several areas; airlines have obligations through their civil aviation authorities (CAAs) – the organisation's own standards are imposed in countries where there is a weak CAA.
    b. Case 2: *no comments.*
    c. Case 3: national and global aviation standards (such as CAA best practice guides) impose the organization to be compliant and include such standards in its CMS; the organization is initiating voluntary regulation as there is no other regulation to follow for certain developments in new areas; adapting existing standards/internal policies; investing time and resources in trying to create what will be the industry standards (in collaboration with other regulating parties); changing industry standards takes forever; considerations around liability; creation of ethics compliance frameworks.
30. The type and form of collaboration with external parties and how it influences, impacts or affects compliance management activities (whether it is vendors, collaborators, partners etc.):
    a. Case 1: thinking about the architecture of the system, where it's going to sit, where it's going to be hosted (user types, countries, nationalities) and kind of impact on the end system – these considerations need to be dealt with together with external parties; collaboration with cloud service providers; pushing

industry standards together with other more influential authorities (with the right power).

b. Case 2: establishing good SLA contracts with providers; regular update meetings; large providers offer a lot of governance; dependency on legacy providers can cause inefficiencies that cannot be avoided.

c. Case 3: the organization must come into agreement with the CAA and other airlines on what it spends money on; collaboration with key clients in setting up pilot projects also known as accelerators, where the client invests in the infrastructure and in start-ups within the organization's environment; collaboration with organizations with similar operations for splitting scenario testing and sharing of lessons learned; collaboration with providers where the organization is doing part of the work as due to safety and security compliance, the third party is not able to i.e. capture enough data (digital images) to teach its system to work autonomously; sharing of best practices and learning the different needs/requirements of similar organizations around the world; collaboration with third parties on joint product offerings, driving people behaviour and the compliance behind it; disseminating compliance internal information/requirements to third parties has to be improved.

31. Topics related to data management, governance, and other considerations related to data within the organization:

a. Case 1: the organization is already using a lot of rule-based applications using structured data (data already existing in a database); robust data management is needed to unlock AI possibilities, building the foundations on how to manage data, structure it, govern it, data leveraging to create applications and building a harmonized ecosystem of data management; in the industry, robotics are not as relevant as data analytics applications; for example the finance function and related processes are well organized and executed, the same organization and process enablement should be adopted for data accessing, as part of its governance; the organization is highly relevant for data processing and data management and has therefore a high concern with compliance; complex decisions and rules need to be considered due to the various jurisdictions, countries with embargo and sanctions topics; design applications from day one (system blueprint design, system architecture: users, countries, nationalities, impact on usability); relevant, quality-checked data is needed to avoid having bias in the decisions taken; avoid algorithms/rules using poor quality data; collect enough data that is representative and sufficient to do proper testing/simulation/digital twin projects; testing compliance and compliance of applications depends on the data quality and amount (the amount of data that will have to be collected will have a direct impact on the quality of the testing); important to bring data together by building a data lake, with a proper governance programme.

b. Case 2: *no comments.*

c. Case 3: collecting sufficient and quality (right) data for the purpose of the pilot projects where automation/AI applications are trialled for feasibility; collaboration in data sharing with third parties – considerations around compliance and data security; data storage and working with cloud providers (Microsoft Azure and related Microsoft Office 365 products for visualization) and decision-making processes).

32. Topics related to information security and how these affect the compliance policies and procedures of the organization:

a. Case 1: cyber security is at the forefront of using AI within the organization, as this is a critical area for the business (examples include monitoring external users entering the system, detecting and monitoring anomalies); compliance management best practice is therefore currently found in cyber security – compliance with information security; testing the system and making the link between system reliability testing, training, results and security implementation based on the findings; implementing mitigation actions; real-time monitoring using dashboard tracking of users, servers, workstation compliance; the organization has cyber security insurance since the potential loss to the organization and its clients is very high (dependency on data, the organization acts much like a bank for its clients); business KPIs reporting (number of security risks - extrapolated from the risk management system, number of security incidents, people KPIs, third party assessment); a lot of compliance needed to meet certification requirements (see impact of global standards results at proposition number 28 above).

b. Case 2: *no comments.*

c. Case 3: compliance of AI applications has to be scrutinized and due diligence applied before selecting a provider; example is a robot available on the market, which the organization tried to start a pilot project with – before the project started, the robot was found to be riddled with security issues, which connected to the organization's network would pose a big risk to the entire firm; security concerns have to be addressed first, and this is done as part of the organization's processes, as the organization is considered national critical infrastructure.

33. The consideration of ethical concerns when elaborating, adopting, operating automation/AI applications/tools:
    a. Case 1: ethics considerations when considering designing systems and data access for different jurisdictions around the world.
    b. Case 2: *no comment*
    c. Case 3: developing an automation compliance framework, based on existing frameworks – additional considerations have to be given to ethics framework as part of it, to address the on-going concerns around ethics of automation/AI etc.; consider what automation/AI means for the community, for the future work, for the environment; sustainability of aviation is a key discussion, and has to be blended with ethics of automation and AI; currently a lot of things don't have an answer.
34. The IT infrastructure (hardware and software) that the organization has, or is about to implement, as this affects the capabilities of the automation/AI applications or tools:
    a. Case 1: cloud computing on AWS (ERP system on AWS); AWS allows for better security with automated security design, automated user provision and security controls in place; world jurisdictions ask for a lot of different compliance requirements, hence need to use local providers where applicable (e.g. using a Chinese cloud version of AWS in China, need for data related to billing and settlement to stay in Russia).
    b. Case 2: group service provider responsible for basic infrastructure; 200-230 applications in operation (e.g. flight, crew, revenue management); application management includes change incidents, change processes, service management; IT application operations are centralized; the organization has a complex IT architecture landscape; processes are defined in SLAs with the providers, with the key compliance requirement to operate the system; relying on the big global distribution system providers (e.g. Amadeus), and trend is to try to shift the monopoly away to direct distribution – here, sales through

Google's travel agencies (Google has a server in the data centre of the organization); limited providers for core operations' applications (e.g. crew management), hence relying on these handful providers; aim is for getting cheaper more flexible systems.

c. Case 3: the organization still has data servers (two servers plus a third virtual node); regarding cloud computing, it is using Microsoft Azure, with some limited applications on AWS; system reliability is the key consideration as the availability of operations data of the organization is critical and therefore a high risk area, which make data management and compliance paramount.

6.2.2. Results: documentation data, analysis and propositions

The types of documents analysed from the three case studies, fall into one of the following categories: code of conduct, online sources (news, press releases), annual reports (online sourced), meeting minutes, organizational charts, job portals (online sourced), company registrars (online sourced), investor reports (online sourced). The matrix of documentation analysed, with an overview and split per case study organization, can be found in Appendix F. This section outlines the results of this analysis, split per case study, and it allows the two sources of data collection (interviews and documentation) to speak to each other.

A limitation of this analysis is the type and extent of documentation available. This is on one hand a consequence of the willingness, time availability and other restriction constraints on the side of the interview research participants. On the other hand, it is a consequence of the amount and type of information made publicly available. These are both factors, which this research cannot control for.

Case 1 documentation analysis

By analyzing the documentation related to case study number 1, the following remarks can be made, regarding how compliance is addressed within the organization:

- A comprehensive code of ethics and business conduct exists.
- The code provides employees with the resources available to address compliance-related questions.
- Online sources indicate the investments in cyber security and digital transformation, and also the push of standards to the wider industry (the key customers/stakeholders of the organization).

a) Code of ethics and business conduct

From the code of ethics and business conduct (Appendix B), the following are results to be discussed further in the "discussion of the findings" chapter.

- Training to employees to understand the code.
- The code is not intended to be all-inclusive.
- Policies are classified according to five categories, and are summed up in a "policy guide": (i) Audit, Legal & Risk Management; (ii) Finance, Administration, Procurement, Planning & Projects; (iii) People, Performance & Development; (iv) Information Technology; (v) Communication & Marketing.
- The organization provides employees with assistance contacts for a list of seventeen questions related to the code's topics or applicable policies (see Table 1.Appendix B).
- Specific compliance programs have been developed by the organization to ensure compliance with applicable laws and regulations.

Resources for assistance: these are the roles responsible for the different policies (see Table1.Appendix B). The list provides both an overview of the organization's existing core policies and about the key contact functions (e.g. assistant general counsel for economic sanctions compliance).

b) Online sources

From the available online sources, the organization's website provided two types of documentation relevant to this research: annual review report for 2019 (see point c below; no details on financial situation of the organization), and press releases (details on managerial restructuring were analysed). The press release (IATA, 2019) announces a newly formed “Financial, Distribution and Data Services (FDDS)” division, which is to group the organization's work on digital transformation, efficient industry processes, product differentiation and business intelligence.

c) Annual report

The organization’s annual report is a complete report on the successes, issues and state of commercial air transport. The analysis focused on the areas concerning the organization and which are pertinent to this research; the results are as follows:

- The organization is working together with industry stakeholders towards information security.
- In early 2020 expected to provide guidelines for a comprehensive approach to cyber security for the air transport industry.

Case 2 documentation analysis

The results here are used in the “Discussion of the findings” chapter in conjunction with the results of the interview data analysis, showing primarily the implications of being part of a group company structure (strengths and weaknesses). By analyzing the documentation provided by the case organization number 2, the following remarks can be made, regarding how compliance is addressed within the organization:

- The parent company (the company that sits above the case study organization) addresses compliance within its “group CMS”.
- The parent has its own “Code of Conduct”, which sits above the subsidiary’s own document.
- The subsidiary (the case study organization) has its own “Code of Business Conduct”, where several aspects of the group CMS can be found (see list of content in Appendix C).
- Data from a sample of meeting minutes of the compliance committee of the organization reveals little about the automation applications in the various areas of compliance. It does however validate parts of the data from the interview with the compliance counsel.

Other sources of documentation included publicly available data, retrieved from online sources such as company websites, jurisdictional company registers.

a) Code of conduct

From the “code of business conduct” (Appendix C), the following are results to be discussed further in the “discussion of the findings” chapter:

- Correlation between CMS and the topics addressed in the code of business conduct exists almost one to one.
- The regulations, directives and manuals of the organization supplement the rules and values specified in the code of business conduct.
- Guidance on compliance with the law due to the international nature of the operations of the organization exists (wide range of legal frameworks and parameters).
- Internal communication and reporting of issues is addressed and guidelines are offered.

b) Online sources

For case 2, it has been found from press release information, that one of the parent’s strategic initiatives when it comes to adoption of AI tools, is the strategic partnership with Google Cloud to use its platform for the following: improve operational performance, minimize the impact of irregularities on its passengers:

> “The aim is to build a platform that will suggest scenarios to return to a stable flight plan in the event of an irregularity. This will be done by merging data from various processes that are relevant for stable operations (for example aircraft replacement and maintenance as well as crew scheduling)” (Deutsche Lufthansa, 2020).

c) Compliance committee meeting minutes

Types of compliance addressed by the dedicated compliance function, as part of its regular compliance committee meetings: competition, integrity, third party due diligence, embargo/export controls, capital markets, other topics (code of conduct, compliance risk assessment). The group CMS is structured in six areas (see Appendix C for details).

d) Organizational chart

The chart of the local group companies says little; it indirectly confirms the enablers and barriers that are faced in light of being part of a large group organization.

e) Annual report

The annual financial report of the organization is not publicly available, yet the parent annual financial report (Deutsche Lufthansa, 2019) (has been analysed with respect to investments in digital technology and to audit costs (costs of compliance monitoring). Additional data has been found related to compliance management within the group. Key results from the annual report are:

- The business processes in the group are supported by IT components in virtually all areas.
- Technological tools have been introduced to prevent cyber attacks, processes have been adapted to changing risk scenarios, organisational changes have been made and awareness campaigns have been carried out.
- The group sources most of its IT infrastructure from external service providers.
- Compliance describes all measures taken to ensure the correct conduct of companies, their management and their employees with respect to statutory and the company's own obligations and prohibitions. The group Compliance Management System is intended to prevent employees and the company from coming into conflict with the law and at the same time to help them to apply statutory regulations correctly. The group compliance programme is made up of the following elements: competition, capital markets, integrity, embargo and corporate compliance.
- Top three quantitative risks for the group are: fuel price movements, cyber and IT risks, breaches of compliance requirements.

f) Job portal

The results of scanning the list of open positions of the organization, speaks to a strategy of investment in automation/AI development, with positions such as "Senior Business Analyst & Data Scientist", "Distribution Application Analyst", "Business Analyst Revenue Management".

Case 3 documentation analysis

By analyzing the documentation publicly available (online sources) with respect to case study number 3, the following remarks can be made, regarding how compliance and automation topics are addressed within the organization:

- The organization is investing in updating key systems supporting the operations, by ensuring these meet compliance requirements.
- Relationships with third parties are key in coordinating compliance activities.
- Data protection is a key sub-function of the legal department.

a) Online sources

The key publicly available information, analyzed here, presents the following results:

- The organization is dependent on its relationship with other partner organizations, which belong to one of the eight categories: airlines, civil aviation authorities, airport coordination, commercial services, revenue & customs, border authorities, air traffic control, public transport operators (Heathrow Airport Limited, n.d.).
- Some of the automation/AI projects deployed, or in trial at the airport are led by partner organizations (e.g. airlines), which means that compliance-related topics have to be coordinated with these external organizations (Airport Technology, 2019).
- In 2019, the focus of the automation activities of the organization were reducing manual handling and bringing more automation into the baggage system, creating an ‘autonomous vehicle ready’ environment at the airport, improving stand efficiency and safety through automation (Robotics and automation, 2019).
- According to the “Investor Report December 2019”, capital expenditure plans for 2020 include improvements in areas that ensure compliance to either external regulations, or safety standards: “Hold Baggage Screening” ensuring DFT compliance, “Main and Cargo Tunnel” works to ensure fire safety standards are maintained (Heathrow Airport Limited, 2019). These areas are all related to the core business of the organization. In addition, the organization deals with aviation business, advertising, ground handling, cargo, flights, parking, business lounge, restaurants, and shops; no further information could be retrieved regarding these business areas belonging to the commercial tier of the organization.

b) Organizational chart

The organisational chart of the legal team indicates the areas of focus regarding legal and regulatory compliance, with legal sub-functions existing for: operations, commercial, infrastructure, data protection, and expansion. Under the legal operations, a dedicated team for regulatory and competition law exists. In addition to these sub-functions, a senior finance counsel has a separate small team, integrated within the jurisdiction of the office of the general counsel.

b) Annual report

From the annual report of the year ending 31 December 2019, there is no information available on the auditor fees, respectively no granularity on the costs related to support functions such as business assurance, nor granularity on investments in technology. The section “capital expenditure” of the report, gives only a glimpse at the investment in automation for the organization’s infrastructure and development (Heathrow Airport Limited, 2020).

6.3. Thematic structuring of propositions

Having outlined the propositions that resulted through the abductive data collection in the “Data collection and analysis” chapter, the research’s findings are clustered under the nine themes below. These themes represent the findings of the research since they have emerged as demi-regularities (patterns found in the results) and are discussed later on, in the “Discussion” chapter. This emergence can be traced back to the categories, codes and definitions (part of the coding process of the data analysis) detailed in Appendix A. As a reminder, the coding process represents the skeleton of this research, the theoretical framework allowing for future generalization to new cases (Yin, 1994). The categories of the coding (Appendix A) are a direct representation of the categories used in the interview questionnaire (see Appendix E) and expand into rationalized codes, leading to propositions. The common attributes of the data clustered under these propositions have blended into the nine themes outlined in this section, and further elaborated in chapter seven “Discussion”. This thematic discussion, mixed with the theoretical background and the conclusion of this research, have led to the recommended conceptual guidelines (see chapter 9) of this research, fulfilling the ultimate aim.

1) CMS components, structure, responsibilities

The CMS components, structure and responsibilities theme encompasses the understanding of the types of compliance addressed by a compliance function within an organization (if one actually exists), the understanding of how compliance is structurally addressed (roles, responsibilities and reporting), as well as the understanding of the design of compliance embedded within the organisation's processes (policies, frameworks and other models). Last but not least, the theme also includes the understanding of monitoring and auditing activities of an organization.

The key topics affecting the research framework of the CMS ecosystem are listed below. These topics have resulted from the case study investigation on how compliance management systems are strategically set-up in organizations, and the degree to which these systems are supported by AI applications. At the same time, these topics are indicative of the conceptual guidelines that will be recommended as an output of this research. The components, the structure and the responsibilities in a CMS have to consider the following aspects within an organization (these findings can be referred back to the results presented under the thirty-four propositions in sub-section 6.2. in this paper):

- The highest focus of compliance-related actions is on the highest risks, or most important business areas of an organization.
- The culture and the risk appetite of an organization are a result of the main purpose of operations, hence stakeholders are the real decision makers when it comes to what, how and how much is invested in compliance activities.
- It is important to assess the structure of the organization and to use this and the overall purpose of the organization to better understand how and where compliance applies (e.g. very different compliance areas for an airport compared to an airline, despite operating hand-in-hand and within the same industry).
- A CMS within an organization should not have a dedicated role for head of compliance (e.g. Chief Compliance Officer), rather the CMS should be embedded within the nature of operations and culture of the organization, and each executive person should have the role of overseeing and contributing to this system. A management system should drive the feeling that everyone owns it and instigate a feeling of responsibility.
- When you have a compliance function, the scope of work is narrow-minded to what the function actually does. Compliance per se goes into every aspect of the

organization and there are already many tools enabling the business and operations to be compliant in an autonomous way.

- A CMS is not a physical system, not even one that can be entirely articulated in a policy, a framework or a manual.
- In order to own processes/activities, employees must be involved and officially empowered within the development and change process.
- Ensure availability of a team of experts, which is ready to offer guidance and explore opportunities on the topics and questions related to compliance management.
- Owners (employees) of emerging compliance topics (e.g. second line of defence) should be accessible to be contacted in analogue manner. Therefore, it is important to balance out what support can be offered through digital/automated tools (best candidates are repetitive tasks), and therefore free up time of those employees for face-to-face availability.
- Offer training to people, into the basics of how a tool functions and makes a decision (explaining the rules and logic built behind it), enabling them to not perform their work blindly.
- GDPR data officer is one of the key roles in organizations today.
- Workarounds for certain cases requires human judgement: e.g. avoiding cumbersome, unnecessary rules to ensure speed of operations. Such situations must be properly assessed. A process is needed to deal with specific cases or with exceptions to the standard compliance process. Considerations have to be addressed, on how to monitor the exceptions handling process.
- Ensure compliance through contingency planning, design the “what-if” scenarios: compliance process of current/desired state, compliance process of scenario states.
- The process of planning the timing and recurrence of communication of emerging rules/legislation/policies has to be compliant to requirements enacted upon the organization.
- First line of defence feeds the second and third lines of defence with best practices: experts within business areas, within operations, are connected to their work’s best practices through their daily activities and through their outside network.
- Decisions on which tasks to automate have to be linked to an organization’s strategy because automation does not always make a process more efficient (e.g. training of employees: if the manual task in question is also a means of training, then the cost of

training might be less than that of automating, and afterwards finding a way to offer training for that computer application).

Quotes from the data collection interviews, related to this theme's findings, can be found below:

> *"One of the things we were looking at was maybe the inclusion of a specialist compliance function. But we think that we can work it better within that management system that would instead of having people just concentrating on those areas to make our model slightly better" (case 3, interview 1).*
>
> *"But I always find that those are really good things for trainees to do because I get a real understanding of whether or not the trainee knows what they're talking about, because it brings it down to a series of questions [...] you can teach a computer to read handwriting and transport it into text [...] but what you can't teach it necessarily to do is sort of run that double check about what is what you're saying" (case 3, interview 1).*
>
> *"We have a data protection officer from our legal department whose main focus these days is probably GDPR and GDPR equivalent regulation in other countries" (case 1, interview 1).*

2) Enablers and barriers of AI

Enablers and barriers of AI is a theme that is related to the second and third research objectives. With this theme, the focus is put on understanding what the forces behind the adoption and use of AI within organizations are, either positive or negative. The research has focused on the basic applications of AI, which includes automation of tasks (a computer software or computer-controlled robot performing tasks commonly associated with intelligent beings). It will be observed within the "Discussion of the findings" chapter, that many of the other identified themes can be considered either enablers or barriers of AI.

The key enablers of adopting AI within organizations, resulting from the findings of this research, are listed below (refer to the results presented under propositions 5 and 6 in sub-section 6.2. in this paper):

- Tools are augmenting the capabilities of people, reducing complexities and eliminating time spent on manual and time-consuming tasks. People can focus on real business activities, where, according to Dwivedi et al. (2019) they have access to a higher quality of information to support decisions.

- Cost is both an enabler and a barrier.
- A strong data management practice is needed to be able to scale the opportunities of AI. As part of a data governance programme, it ensures among other things, that sufficient and right data are available to the organization to feed its AI applications.
- Senior management support is paramount in creating internal capabilities for deploying AI.
- Regulation for new technology (e.g. AI applications) forms industry standards, and is likely to drive a higher and sooner adoption of such technologies.
- AI can make it easier for people to comply, helping e.g. managers to take decisions by themselves, simplifying internal processes.
- A large group organization possesses economies of scale, which could enable the adoption of AI within the organization.
- The improvements in quality of products, services and customer experience offered to the clients are an enabler of investment in AI.
- The increased employee well-being by adopting AI that supports the work of personnel is also considered an enabler.
- Reduction in FTEs is an enabler (e.g. in operations areas where dependencies on humans can cause delays or system interruptions).
- The chance to employ adaptable AI applications with data interpretation capability and capacity.
- Breaking out the linear relationship between OPEX and CAPEX.
- New infrastructure developments enabling automation are: computing capacity, both cloud computing and edge computing capacity (computing capabilities to process large volumes of data in real time); network connectivity.
- Good results from e.g. pilot AI projects show the benefits of AI applications and hence drive demand for more AI-driven solutions across the organization.
- In certain cases, legal requirements make it imperative to adopt AI solutions, this being an enabler for early adoption.
- Safety and security requirements can also enable the adoption of AI applications.
- The understanding of processes, of dependencies, of compliance requirements, in an organization is very important and it enables adoption of AI.

- Cross-industry collaboration and sharing of lessons learned enables adoption of AI.
- The change in the easiness and the costs of implementation of AI applications is considered an enabler.

Quotes from the data collection interviews, related to this theme's findings, can be found below:

> *"Cost is obviously a massive driver. You know if we could use an AI system that involves us, reducing the number of people that we have to employ to do something, then that's really important. It sort of comes down to cost basis at the end of the day, but it also comes down to satisfaction with the airport" (case 3, interview 1).*
>
> *"The foundation of data management is key to unlock AI possibilities [...] There's going to be an accelerated move towards strong data management (enterprise-wide) practices with good facilities in terms of storage" (case 1, interview 1).*

The key barriers of adopting AI within organizations, resulting from the findings of this research, are listed below:

- A weak or inexistent data management practice within organizations.
- Heterogeneous IT application landscapes in organizations can be barriers to the adoption of AI.
- Cost is both an enabler and a barrier.
- Regulations for new technology (e.g. AI applications) would form industry standards, and would likely drive a higher and sooner adoption of such technologies. While this can be an enabler, at the moment is more a barrier since in many AI development areas regulation is inexistent or unfit for purpose.
- The high level of due diligence required in adopting AI, makes due diligence a barrier.
- The more stakeholders involved in a given context, the more compliance requirements exist.
- The higher the number of stakeholders who have a saying in decision-making, the higher are the barrier in adopting AI applications.
- Monopolistic distribution channels for products or services can impede or delay the adoption of AI applications.

- Slow decision-making processes can make AI technology obsolete by the time approvals are obtained and computer applications become operational.
- Changes in liability when relying on automation make the adoption of AI to be more cumbersome.
- There seems to be a fear that innovation does not lead to an asset.
- Resistance to change by employees is a barrier to AI adoption.
- The fear of ending up in the control of computer programs or algorithms, of binding to a system without alternatives, is a barrier to the adoption of AI.
- Safety and security compliance requirements also represent hurdles to innovation and therefore can be barriers to the adoption of AI.

Quotes from the data collection interviews, related to this theme's findings, can be found below:

> *"So we're now investing, you know time and resources in trying to create what will be the industry standards" (case 3, interview 2).*
>
> *"There's the monopolist (distribution application) [...] you have no advantage from it, you know, when some booking comes from some tour operator, who have (distribution application), you have to pay" (case 2, interview 2).*
>
> *"Lots of innovation there's a chance that whatever you're innovating doesn't become an asset" (case 3, interview 2).*
>
> *"I think there is still a little bit of fear with some people that if you put your hands and put yourself in the arms of computer programs or algorithms or whatever it is, then, you can come untuck and if you don't have a good sort of manual process to fall back on" (case 3, interview 1).*

3) Control and compliance of AI applications

The theme discussing the control and compliance of AI applications is one that touches on the implications of trusting computer software (AI applications) and how this can be achieved, therefore having control over the input, processing and output of such software, and therefore ensuring compliance. The theme was born out of the data collection discussions with interview partners, as well as out of the enterprise-level view of a CMS, where those applications enabling the CMS must be, at their own end, compliant with (adhere to) internal and external regulations and standards. The theme also relates to one of the categories of subjects presented in the literature review, that of governance of AI.

As argued in the literature review, being equipped with the right understanding of AI applications, and at the same time having the legislation in place to regulate AI-driven processes is what is needed by a governance programme of AI. Ultimately, this gives a level of control on AI applications by demonstrating compliance to sound policies/legislation/standards and hence reduces the risks posed by AI-driven processes, enabling processes at their own end to be compliant. This area falls under the responsibility of the second and third lines of defence and it impacts the monitoring activities within the CMS ecosystem. At the same time, the theme must be located under the umbrella of IT governance within the wider corporate governance topic. Here, the fourth line of defence (as introduced earlier in chapter 2.3.) represented by the board and the regulatory supervisory bodies, is responsible to determine who makes the decisions within the system of AI applications, and who is responsible and accountable for making and implementing the decisions To the help establishing a system for ensuring control and compliance of AI applications, ISACA is the body responsible to provide the standards for information governance, control, security and audit professionals (ISACA, 2021). It is under this constellation, that organizations can tackle the following subjects when it comes to control and compliance of AI applications.

Key topics to consider towards achieving control and compliance of AI:

- A new area of compliance preoccupation needs to be factored in the CMS: compliance of the algorithms/rules used by or embedded within AI applications, either for business processes or for enabling compliance management processes.
- Raise the question on how liability will change when automating.
- Build systems/tools/applications that have reliable, comprehensive and simple manual/fall-back steps, processes that are redundant to people interacting with it (including the right set of controls).
- Audits are needed even for mature real-time monitoring systems, as these systems have to be audited / checked against what they are doing (e.g. actual output vs. expected output).
- Sufficient and unbiased data will have a direct impact on the quality of testing applications, and therefore on the quality of the subsequent compliance of the systems put in production.

- Data is used both by business use case applications and by compliance-support AI applications. Compliance-support AI applications provide automated support in the compliance adherence process and the monitoring of this adherence. At the same time, compliance-support applications should support the checking of compliance of source data.

Quotes from the data collection interviews, related to this theme's findings, can be found below:

> *"When everything is autonomous pedal never bumped into itself...while again that's part of the bit that needs to be worked through the regulations and a lot depends on what has the market develops but Volvo have already come out and said that they have an autonomous vehicle [...] and they're going to be liable" (case 3, interview 2).*
>
> *"The process should be engineered in such a way that there is redundancy. And there is, you know, conflict of interest is managed" (case 1, interview 1).*
>
> *"That new compliance preoccupation will come when we will look at the algorithms for that being created with the machine learning. And this, the solution would be probably the software development lifecycle. Because the testing methodology will be totally different" (case 1, interview 2).*

4) Compliance by design (CbD)

A key theme in the research, CbD is a recurring topic in the conversations around any new development, be it of a product, a service or a process. The considerations of the elements that make products, services or processes compliant from day one can be of outmost importance in achieving a CMS that is enabled by AI. This can be true partly due to the fact that computer software tasked at informing the human is more likely to be doing the right thing and actually helping the adherence of a business process to whatever it has to adhere to.

The theory resulting from both literature and findings indicates the following aspects that have to be considered when it comes to embedding, as early as in the design phase, compliance requirements within processes or applications:

- Designing a CMS (and affiliated policies, procedures, manuals etc.) should be done in a user-centric approach, and hence make it easier for people within the organization to be compliant than non-compliant, then half the "compliance battle" is won.

- In order to own processes/activities, employees must be involved and officially empowered within the development and change process.
- Involve all stakeholders by making sure all their worlds are met (all requirements), consensus is met where conflicting needs cannot be simultaneously designed.
- Build systems/tools/applications that have reliable, comprehensive and simple manual/fall-back steps, processes that are redundant to people interacting with it (including the right set of controls).

Quotes from the data collection interviews, related to this theme's findings, can be found below:

> *"If you make it easier for people to be compliant than not compliant, then that's kind of half the battle won, right" (case 3, interview 1).*
>
> *"Create a systematic risk and compliance ecosystem, that's driven by deterministic and rule driven can engineer your compliance process rather than relying on people because people by definition, they are prone to making mistakes, they're prone to have conflict of interest they are prone to fraud, and less so if you have an engineered a system that is resistant to these aspects" (case 1, interview 1).*

5) Data governance and data management

The theme of data governance and data management has been identified as a driving force towards adopting AI applications. It is a building block for a digital enterprise and as such can be either a key enabler or a key barrier towards successful deployment and operationalization of AI within an organization. Data governance specifies a cross-functional framework for managing data as a strategic enterprise asset by formalizing data policies, standards, and procedures and monitoring compliance (Abraham, Schneider, & vom Brocke, 2019). Some of the underlying topics within this theme are data sources, data from various processes, data protection, data security and adoption of cloud platforms for analytics.

The initial theoretical CMS ecosystem (framework) has indicated two sources of data within organizations. These, combined with literature theory and empirical research data, have provided the following key considerations regarding data governance and data management. At the same time, recent theory investigation suggests these considerations make the case for considering the theme as an essential element in designing an enterprise CMS. The key considerations are:

- Data protection and cyber security are probably the two most important areas of concern for organizations today. Hence data governance, data management and information security compliance should be high on the agenda of executives.
- Ensuring that data is compliant with the governance programme is crucial in today's digital world, and in planning for the future (cross-data-management).
- For the purpose of pilot projects where AI applications are trialled, sufficient and quality data needs to be collected and made available, often to third parties. Therefore the rules set by a data governance programme should address data sharing and security considerations.
- Enterprise-wide AI-enabled CMS starts with an enterprise-wide data management ecosystem.
- The following will have a direct impact on the quality of applications testing, and therefore on the quality of the subsequent compliance of the systems put in production: sufficient data and unbiased data.
- GDPR data officer is one of the key roles in organizations today, responsible to disseminate the compliance requirements within the different business areas of an organization and monitoring the compliance with data protection regulations.

Quotes from the data collection interviews, related to this theme's findings, can be found below:

> *"In order to test your algorithms, you will have to collect enough data that will be representative". "The biggest value is really the creator of the data. So, if you have the right data. Normally, would be quite easy to implement the different algorithms for the machine learning (case 1, interview 2).*
>
> *"We also connect directly, Google, for example, directly connected they have a server in our data centre" (case 2, interview 2).*
>
> *"Data privacy was a big component something that we had to bring out last year to be brought in line with the new GDPR provisions. And the way that we did that we have, we have a team of four people within the legal team that deal with data protection issues, and they liaise with data protection champions within the business who then have the responsibility for going or the accountability for going into their areas of the business and making sure what they do is that is compliant with data protection regulations" (case 3, interview 1).*

6) Cyber security

The security of information and of other communication and automatic control systems is a topic gaining the attention of all stakeholders of organizations relying on information technology, and as such, it has been identified as a theme to be discussed in light of the results of this research. The subject has also indicated that, due to the high risk of IT security breaches, cyber security compliance has received a high level of attention and therefore investment, resulting in it being at the forefront of AI adoption and therefore driving best practice in the use of AI.

The results of this study indicated that the security of information and of other IT systems, represent a priority for organizations. This is due to the fact that the core business operations and therefore business continuity, relies on these systems and embedded information. As such, the investments made in augmenting the compliance requirements in this area with AI applications, is significant and ahead of other areas. These are the key general take-away points from this research:

- Data protection and cyber security are probably the two most important areas of concern for organizations today. Hence data governance, data management and information security compliance should be high on the agenda of executives.
- Cyber security is often best practice when it comes to compliance management.
- AI is needed in cyber security to deal with the large amounts of data and data sources, making the monitoring process more efficient, allowing employees to focus on matters requiring human interpretation.

Quotes from the data collection interviews, related to this theme's findings, can be found below:

> *"The three pillars of dealing with cyber security, and the risks of AI components put in place to detect where things are happening, what are threats, and so on, but not so much on tracking regulations. We don't have AI tracking, you know, state specific, you know, regulations on data protection and things like that. It's done manually (case 1, interview 1).*

> *"Artificial Intelligence is already a must. Because you will not be able to deal with the volume and the complexity of what you receive issue, while not adding artificial intelligence tools to, to make it simpler hackers are using robots to attach us. We have*

> *to use robot to defend us. And so it becoming robots against robots" (case 1, interview 2).*

7) IT infrastructure (software and hardware)

The IT infrastructure of organizations, composed of both tangible (hardware) and intangible (software) assets, represents a driver in the pursuit of using technology applications such as automation or AI. The data analysis has indicated in numerous occasions that this is a theme of importance in the context of this research, and therefore shall be included in the discussions of the findings.

When it comes to the infrastructure supporting the deployment of AI applications, both software and hardware play an equivocal role. This research has found that the following points shall be covered in order for organizations to be able to tap on the opportunities offered by AI applications:

- New infrastructure developments enabling automation are edge capacity (computing capabilities to process large volumes of data in real time) and network connectivity.
- The speed and easiness of IT implementation projects has increased and therefore make it more likely and feasible for organizations to engage in such endeavours.
- Cloud computing and entering new partnership programmes with large technology providers enable the strategy of AI adoption in organizations, by eliminating the high investment costs that would otherwise go into physical infrastructure (e.g. servers).

Quotes from the data collection interviews, related to this theme's findings, can be found below:

> *"Machine analytics, camera analytics have been around for years. But you've never either had the edge capacity to be able to process them or the network to be able to get them back and so I think finally you're getting the overall ecosystem that you can then start plugging all of these things in in together" (case 3, interview 2).*

> *"We have been with Amazon Web Services for more than 6 years. Yeah. And I have better security now, because I was able to automate all the so we did the security design before. And then after we were able to implement, and all the new physical every time that we create a new virtual machine. It is us doing it it's not the user. So, the user is not allowed to create his own account and his own machine" (case 1, interview 2).*

8) Regulation and regulators

Regulatory bodies, at both local and global levels are in one way or another driving compliance management within organizations. Two areas within this theme have prevailed from the data analysis, which are the relationship of organizations with regulators, and the global and local standards. The first area shows that the design of a CMS's elements is correlated to the outputs (the work) of the relationship with regulatory bodies. The second area indicates how certain elements of a CMS are a direct consequence of existing global and local standards, which cannot be circumvented.

The demi-regularities encountered in the empirical data are supported by previous research findings, Parker (2003) suggesting enriching the "management-compliance program-corporate performance" chain by creating loops in the communication of audit results between management and regulator, and not just pushing the audit report to the regulators as a mere statement. The findings of this research suggest the following points are also key in supporting an enterprise-wide AI-driven compliance management system:

- The relationship with regulators is what drives the development of policies.
- Industry standards are a good method of "operationalizing" compliance activities and also to drive the investment in reducing the compliance efforts.
- Examples of industry standards are ISO standards, standards specific to industries such as aviation resolutions and recommended practices.
- Industry-dictated standards drive compliance activities and subsequently drive the training curriculum of auditors' skills and competencies.
- Regulations can put hurdles to innovation, so that, for example, achieving augmentation/automation in another part of the business (which enables compliance), can take a long time and requires a high effort.
- For new areas of development, collaborating with the regulatory bodies to create industry standards means speeding up things and gaining common results.
- If regulations would exist for new technology (e.g. AI tools) and would form industry standards, they would likely drive a higher and sooner adoption of such technologies.

Quotes from the data collection interviews, related to this theme's findings, can be found below:

> *"So we then start thinking well okay we need to start working with all our regulatory bodies. So as you know, IATA which is the airline regulatory. There's ACI, which is the airport one then ICAO over data standards" (case 3, interview 2).*

> *"We have some process, and we have also some reports, and the internal audit is able to investigate and to have access to all our security tickets and to and to verify that we comply with, you know, the cyber security programme that we have auditors that have been trained on information security or SOC 2 or PCIDSS" (case 1, interview 2).*

9) Collaboration with external parties

The last identified theme in the data analysis phase, has been the collaboration with external parties (be it suppliers, business partners, clients, competitors, industry players). In a nutshell, the collaboration with those parties belonging to the ecosystem in which the organization is operating and active. The collaboration can support and enable faster advancements and developments in adoption of automation and AI.

Clearly the results of this research point out to the fact that an AI organization (be it a data science, machine learning or a hybrid) is dependent on external parties to succeed. The key points to consider in the collaboration with external parties are:

- Reliance on third parties cannot be downplayed (e.g. for development, maintenance of IT infrastructure), hence SLAs are of utmost importance for compliance management.
- The first line of defence feeds the second and third lines of defence with best practices since experts within business areas, within operations, are connected to their work's best practices through their daily activities and through their outside network.

Quotes from the data collection interviews, related to this theme's findings, can be found below:

> *"We will work off similar systems. So when we think so when they're procuring new screens etc. in the in the tower. […] We will they will put a requisition to us and we'll pay for it. But as we pay for it we need to have the date downloads and the analysis between those things as well so we can run our business so there is there is good interface there between the set-ups what they put in and what we have operationally as our own business as well" (case 3, interview 1).*

> *"Training coach I mean, some of the things that that come through you've got some of the experts in their fields working in these areas. And, you know, you couldn't*

necessarily train some of these people to be higher because they're already talking to the other experts at every other airport around the around the world about what to do in relation to this area and what the best practice is" (case 3, interview1).

7. Discussion

The research propositions and themes are all contextually grounded and theoretically relevant. They speak to both the theory resulting out of the literature review, and the data collected as part of this study. From a theoretical point of view, the discussion part of the research findings is two-folded: (1) thematically addressed; (2) discussed at the three lines of defence levels. This approach allows the discussion to be contextually grounded (themes) in the collected data, and also to be related to the relevant theory presented in the "Definitions and theoretical background" chapter (e.g. the three lines of defence model as a framework of analysis for enterprise-wide management topics in organizations). At the same time, the discussion goes back to the reviewed literature, by linking the results of this study to the six categories presented earlier in this paper. This theory is supplemented in the first part of this discussion by an overall picture of the CMS ecosystem, outlined below under "theoretical framework".

From a practical point of view, this chapter is split in five parts: (1) theoretical framework, (2) discussion based on theoretical background, (3) discussion based on thematic results and recent theory, (4) recommendations, and (5) limitations and recommendations for future research.

7.1. Theoretical framework

Throughout the processes of both writing up of the theoretical background and the literature review, an inductive process has begun, through which the literature has informed the theory on compliance management as a system. The outcome of this process has informed the data collection phase by drawing the CMS as being an organizational ecosystem, defining what compliance means in the business context, and listing the core elements of a CMS. Presented below is this theoretical framework consisting of: CMS as an organizational ecosystem, business context compliance, and elements of a CMS.

1) CMS as an organizational ecosystem

A system of compliance management within organizations can be named an organizational ecosystem. First of all, compliance exists in the business context, and secondly, within this context its theoretical elements allow organizations to make compliance management an ecosystem across the enterprise. A graphical depiction of how this theory could be represented can be found in Appendix G (CMS ecosystem understanding resulting from literature review).

2) Business context compliance

Compliance in the business context is the process of ascertaining the adherence of business processes and applications to relevant compliance requirements, which may emerge from laws, legislation, regulations, standards and code of practices, internal policies and business partner contracts (Elgammal et al., 2016). From this definition, we deduct two streams: (1) subjects an organization must be compliant within (business process compliance, application compliance); (2) activities a CMS must address: (a) emergence (e.g. how to manage emerging compliance requirements, which business unit has to respond); (b) adherence (ensuring both business processes and applications, adhere to the defined, accepted, communicated and implemented parameters). These streams allow to position compliance management across the entire organization, and not only within the typical known legal or compliance business functions or units. This is achieved by understanding that emerging requirements an organization has to comply with can occur in every single area of the organization, and at the same time the entire catalogue of business processes and applications of the organization can be subject to one or more of these emerging requirements. Important to note is the fact that emerging compliance requirements eventually become requirements that are applicable for either a limited or an indefinite period of time, hence they can cease to be associated with the word "emerging", and become simple applicable "compliance requirements".

3) Elements of a CMS

Within this business context, the core theoretical elements of a CMS, matching Willging's (2014) elements, are: (1) training, (2) policies and procedures, (3) internal review and audit protocol. Another way to look at the organization is through the lens of the three levels of efficiency in an organization: workstation, process, and organization.

Going a step further, one can integrate the three elements of a CMS, with the three levels where efficiency shall occur, as proposed by Pawłowski et al. (2009), and then map to the three lines of defence of an organization. The result of this mapping becomes:

1) Training – Workstation – First line of defence (core business units)
2) Policies and procedures – Process – Second line of defence (oversight/support functions)
3) Internal review and audit protocol – Organization – Third line of defence (independent review, internal and external audit)

Within this context, the ecosystem starts with the above three levels or lines of an organization and the dynamics of the interactions among them. The workstation (first) level will be fed with policies and procedures by the process (second) level (through different forms of training). At its end, the process level will own the two subjects of compliance (business process and application compliance) and will have to rely on the two sources of data: (1) internal data information management, and (2) external knowledge management. Both these two sources of data represent input to either humans, or potentially to software (AI applications). Risk intelligent organizations ideally use a tool or a collection of tools (e.g. software as a GRC tool) to achieve alignment of the organization's objectives to the risk-based compliance, by building hard-coded rules within this tool. Rules are nothing else than a set of steps taken when coding, to reach the specific goal of being aligned with predefined objectives of the organization. Within a CMS, the organization (third) level is responsible for overlooking the good and continuous function of the work of the first and second levels (workstation and process). This responsibility is exercised through three types of monitoring activities: (1) monitoring what the workstation is doing with the information provided by the second level, (2) monitor how the second level policies and procedures are transmitted to the first level and (3) monitor how the second line is responding to existing and emerging compliance requirements and what it does to enact these requirements.

7.2. Discussion based on theoretical background

The interviews and other case study data collection, have been driven by the investigation on what makes a set of detailed methods, procedures and routines, that support an organization to manage the business processes' and applications' adherence to internal and external requirements that emerge from different sources, both internal (data and information management) and external (knowledge management) (see literature review for the definition of a compliance management system). As previously mentioned, this set of detailed methods, procedures and routines has three core soft elements, which can be linked to the three levels of efficiency of an organization, as well as to the three lines of defence of an organization: (1) workstation / first line; (2) process / second line; (3) organization / third line. In the next part of this chapter, the results of this research are put into the context of the latter.

1) Workstation – first line of defence

Results from the case study organizations show that the ultimate responsibility for decision-making lies with the business units, which are provided with the second line of defence resources needed to ensure compliance requirements are met. Such resources are account managers from functions such as legal, risk, compliance management, information technology: “if you're looking for example, at legal, I have a legal account manager, who is my go to specialized in my area.” (interview partner 1, case 1). This finding indicates that the theoretical framework presented earlier in this chapter holds true, with the first line of defence (workstation) receiving support from the second line (process). At the same time, enforcing responsibility on the first line of defence can be beneficial to naturally embedding ethics into an organization’s CMS. This individual compliance to regulations and proper risk assessments has been argued by Pérezts & Picard (2015) as being influenced by the ethical judgement of those individuals performing the activities. Therefore, if those people taking the front-line decisions hold responsibility and are correctly supported by timely and accurate requirements (existing compliance requirements), they will use their own ethics in acting lawfully. Together with the second line they will be contributing to the business process adherence to the enacted compliance requirements. This remains a discussable topic, since the human thinking and respective understanding of ethics will be subject to predictable heuristics and biases (Langevoort, 2002), hence the culture of the organization and the tone at the top will likely be influencing the expected ethical behaviour of the first line of defence.

Another finding in the results of this research shows that training is provided to the first line of defence by the second line, results providing examples in the areas of security awareness and compliance or training for the different CMS elements. These examples also indicate that nowadays training is done primarily via online platforms that are set up internally by organizations to meet their individual requirements. Looking at the theoretical framework depicted earlier, where the first level is where training happens, training being enabled by the second line, it is fair to conclude that this framework holds true. Bringing these arguments together, we can see how some form of automation, if not even AI, is supporting this particular part of a CMS: training of policies and procedures offered to the workstation by the process level responsible for emerging and existing policies and procedures.

When it comes to use of AI/automation applications, results of the study indicate that the first line is equipped with an increasing amount of tools that enable employees to make use of information made available though data transformation or algorithms (e.g. operational dashboards, applications with decision tree logic built behind for hospitality or cargo embargo compliance). Within those organizations with operations highly dependent on automation systems, the first line of defence is already extensively augmented by automated systems, such as terminal usage prescription, flight planning, crew resource management, and flight paths prescription. These examples of applications are using not just predictive mathematical models, but go on to use prescriptive mathematical models where people are being informed on the best course of action and remain the "human in the loop" in taking the final decisions. What this tells us is that in order to take the right decisions (in such a case where the information provided by the AI application is considered compliant), humans must trust the application providing the suggested course of action. Trust can be achieved through the concept introduced by Barredo Arrieta et al. (2020), where AI applications are implemented as "responsible AI" and therefore providing an easy understanding of the fairness, the explainability and accountability of the applications supporting decision-making.

On the topic of "Compliance by Design (CbD)", results show that the first line of defence is equally responsible to align with the second line of defence, in addressing both business and IT requirements in IT applications. At the same time, project processes are closely managed and driven by the business side (first line of defence). Considering that the second line is responsible for making available the emerging and existing compliance requirements within policies and procedures, then when engaged by the first line in designing requirements it has to be the driving voice of the requirements to be designed within either applications or business processes. Since the newly designed applications and business processes might at their own end bring up new requirements, these will influence the existing or new policies and procedures, hence CbD is a pre-requisite applicable to these very policies and procedures as well. Attention has to be given to project deadlines imposed by regulators, which can be detrimental to achieving CbD in IT implementation projects (Gozman & Currie, 2014). This issue can further lead to efforts in meeting compliance requirements, being duplicated and scattered across business silos (Volonino et al., 2004), which in turn speaks to the issue identified earlier in this paper of silo compliance.

2) Process – second line of defence

The research has found that organizations empower their business units, and tend to allocate compliance or risk managers/champions to those units that exhibit higher risks. This finding is in line with the literature on risk-based compliance, where organizations tend to focus on the key risks and respond with compliance requirements in those areas, while putting fewer accents on compliance within the assessed less risky parts of the business. At the same time, results show that data protection officers, addressing GDPR among other things, exist in all three organizations. These officers are being involved in all aspects related to data protection, such as new projects, operations etc. These findings reinforce the theoretical framework of the CMS ecosystem introduced earlier, by accentuating the relationship and responsibilities between the first and second lines of defence within organizations. It also reveals the importance of data governance as a strategic item for the top management, since meeting the requirements of the regulation for data protection needs to be embedded in the ways data is managed within the organization.

It has also been found that legal and compliance counsels act as the responsible parties in disseminating emerging compliance requirements. However, compliance requirements that are not part of the organization's defined CMS framework (e.g. IT requirements, finance and accounting requirements) fall in the responsibility of those other support functions. To exemplify this, it has been found that if a new accounting standard is introduced, it is not the task of a compliance counsel to know about its emergence and ensure that adherence to it is achieved, but it is the finance function's task to coordinate meeting the requirements and being compliant. That being said, CMS frameworks in organizations tend to be limited, in scope, to the key risk areas of an organization. The results show main elements of a CMS to be integrity (anti-corruption, anti-bribery, anti-money-laundering), competition, embargo/export, capital markets, third party due diligence. Considering the above, it can be deduced that current versions of CMSs in organizations do not necessarily consider all facets of compliance management as defined in this paper, and as such, they are not spread within all business units to cover all applications and business processes that must be compliant in one way or another. Looking at the theoretical background presented in this paper, the idea of implementing a GRC tool to support the CMS at an enterprise level seems to be a feasible approach. By organizing risk management efforts and providing a uniform view of information, a GRC tool can align risks management with objectives, while harnessing technology (Tadewald, 2014). Of course Bamberger (2010) is right in being sceptical of the blind reliance on tool-based GRC decision making, but making use of such a tool is recommended if this tool is designed with CbD principles in mind, proper training over it is ensured by the second line, and the right documentation on the rules and logic built within is available (to satisfy the need for "responsible AI").

According to the results of this study, policies within organizations are classified into categories that address the different business areas and functions. Examples of policy categories include: audit, legal and risk management; finance, administration, procurement, planning and projects; human resources; information technology; communication and marketing. These policies represent the internal communication of emerging compliance requirements, requirements that can emerge from both internal and external sources. Results from one of the case study organizations indicate that policies and procedures are designed in collaboration with the first line of defence: “That's really important certainly when we design our policies and our procedures. They are not done by legal team or a business team working in isolation.” (interview partner 1, case 3). This finding is in line with the previously discussed topic of CbD and the fact that policies and procedures have to be adapted to the most up-to-date compliance requirements, and at the same time, they have to enable people (while executing business processes) and applications to be compliant: “If you make it easier for people to be compliant than not compliant, then that's kind of half the battle won.” (interview partner 1, case 3).

The results of the research show that for some compliance requirements (e.g. to IT standards), the second line of defence is responsible to ensure the organization is achieving compliance, to train people on IT security matters and also to ensure internal auditors have the training required to perform the necessary audits. This means that the second line is the owner of the applications and underlying procedures, ensures these applications are being used according to their designated policies, and provides training to the first line (the users of the applications), all while ensuring that the independent assurance by the third line (the reviewers/auditors of the applications) is conducted by people with sufficient knowledge of the CbD requirements build within those applications.

Another interesting finding is that monitoring is not only a responsibility of the third line of defence, but also of the second line. Results show how in the case of monitoring access control or workstation compliance, security operations centres are responsible for continuous monitoring, with the third line of defence offering assurance on the correct monitoring procedures and results. This indicates a set-up where the second line of defence is enabled by AI applications (policy compliance tools) in transmitting and enforcing procedures to the first line. Such an interpretation fits well with the findings in literature, which argue that an effective compliance program consists of a culture and infrastructure of compliance, and a compliance IT system (Kim & Kim, 2017).

3) Organization – third line of defence

Two of the case study organizations interviewed, have indicated that their cultural mind-set is not to accept risk, but to mitigate it, and therefore this company value is embedded in company messages, policies and ways of working. At the governance level of an organization, where compliance risk management drives efficiency, over-compliance is represented by a simplified efficiency equation (Horne, 2016) that looks like this: “resources > requirements”; that means that the organization is consuming more resources than what strict compliance requirements would need. With these results and the discussion on efficiency, measuring the amount of resources consumed by organizations in order to not accept risk, but mitigate it, despite potentially being over-compliant, could help better understand the benefits of investing in CMSs that are to some degree enabled by AI. Achieving enterprise compliance requires however elements such as compliance values, managerial oversight and planning, and not just organizational resources (Parker & Nielsen, 2009).

Looking at the responsibility of the third line of defence in the context of compliance management, this lies primarily in its monitoring capacity. Langevoort's (2002) study mentions the fact that human monitoring is using cognitive shortcuts to cope with the vast amount of data that has to be processed, while computer-monitoring systems are able to deal with entire populations of data. Findings from the second case study organization indicate that by using AI in data monitoring (e.g. anomaly detection), humans can now use their cognitive skills to focus on other more soft tasks that cannot currently be programmed into an algorithm. The findings also indicate that the AI applications used in this sense are under the responsibility of the second line of defence (as discussed previously). To support and enable the third line of defence in its monitoring activities, a GRC tool would likely be a way to address this from a technical perspective, where the third line would have available all the information recorded within this tool and would therefore be able to audit it. The tool would help solve the problem of information asymmetry between different stakeholders the organisation has to deal with (the problem arises due to issues in dealing with firstly the complexity and scope of the global regulatory environment, and secondly the actual business operations data) (Butler & McGovern, 2012). Therefore, the auditability of information will be enabled through the audit logs, which the third line would then have to be able to follow up on, and demonstrate the enforcement of compliance within the organization’s IT system (GRC tool) (Ramanathan et al., 2007).

If we look at the governance of AI category in the reviewed literature, one of the key concerns related to AI refers to ethics and the previously discussed concept “responsible AI”. Russell et al. (2010) have a concluding subchapter, where they briefly discuss what the ethics and risks of developing AI are. Out of the six issues addressed, the loss of accountability is the biggest risk faced by an organization willing to deploy AI in its compliance management activities. It can be argued that accountability and respective liability can be transferred from an individual level, to an organizational level, which then in turn leads to other form of compliance to the newly formed rules. This could help answer one of the concerns raised during the interviews, on the unknown elements on how liability changes when using AI applications, which brings up all sorts of ethical dilemmas. When it comes to sound regulation, it has been seen both in literature (Wright & Schultz, 2018) and in practice (collected data), that regulation is lagging behind, and therefore effective governance of AI is still immature: ”changing industry standards takes forever […] we tried to comply to existing regulation when it doesn't really make sense” (interview partner 2, case 3). Being equipped with the right understanding of AI applications, and at the same time having the legislation in place to regulate AI-driven processes is what is needed by a governance programme of AI. Ultimately, this gives a level of control to the third line of defence, on AI applications, by demonstrating compliance to sound policies, legislation, standards and hence reduces the risks posed by AI-driven processes, enabling processes at their own end to be compliant.

7.3. Discussion based on thematic results and recent theory

The discussion within this section goes along the lines of the thematic results of this research. It argues how these themes together with the underlying CMS ecosystem, are affected by recent theory (theories and concepts developed in the stages of retroductive argumentation from phenomenon and causal powers analysis). The theory interrogated upon the data collection and analysis phases, has indicated little new literature on the topic of Compliance Management Systems, compared to the exponential increase in new studies on the topic of governance of AI and other IT infrastructure-related research (e.g. cloud computing, cyber security).

The results show how the different output themes of this research are interlinked among each other, together forming a support framework for a CMS. They appear to be like a web of linked connections, which ultimately meet the purpose of an organization to deploy applications that augment decision-making to an extent to be used in real-life applications at the maximization of the vast availability of data sources (Farrow, 2019). The nine themes in which the results and findings of this research are classified, are: (1) CMS components, structure, responsibilities, (2) enablers and barriers of AI, (3) control and compliance of AI applications, (4) Compliance by Design (CbD), (5) Data governance and data management, (6) Cyber security, (7) IT infrastructure (software and hardware), (8) regulation and regulators), and (9) collaboration with external parties.

1) CMS components, structure, responsibilities

Considering the points brought up in the results chapter of this paper, the theme encompassing the components, the structure and the responsibilities in a CMS sheds light on key considerations affecting these topics in an environment increasingly enabled by AI. One of the findings from the results of this research, has been the need of organizations to offer training to its employees into the basics of how a tool functions and how it reaches a decision (explaining the rules and logic built behind it), enabling people to not perform their work blindly. Interestingly, this view is not solitary, with others arguing that being AI literate ("invoking and putting into practice the most recent AI developments"), requires people to learn "how analytical decisions are made by cognitive technologies and work out how to integrate the analytical capabilities offered by these technologies into organizational processes" (Jarrahi, 2018). Combining this need of understanding with another recurring theme, of CbD, it can be deduced that the process of understanding the mechanisms behind AI applications begins in the design phase of applications, processes, policies and procedures. This also means adapting or creating new policies and procedures by the second line of defence, in strict collaboration with the first line. Sticking to the topic of training offered to employees, the CMS ecosystem resulting from the literature review phase, indicates how the first line of defence (the workstation) is to be given training with regards to emerging compliance requirements. The results from the case study data analysis are supportive of this theory, and accentuate the fact that the first line is trained on compliance topics in various ways (e.g. e-learning, account managers providing both organized and ad-hoc information sessions on emerging issues, training to employees to understand the code of conduct and where to seek assistance). Findings from the documentation analysis (cases 1 and 2) accentuate the subject of training and communication related to the code of conduct, with the second line of defence pointing out the key resources available for assistance (contact functions and core policies associated to these functions). This is an indication of the fact that senior management is trying to ensure that employees and other stakeholders take cognizance of the compliance requirements existing across the various functions within the organization. All in all, both research findings and literature, support the theoretical framework introduced at the beginning of this chapter, even more so when it comes to adopting AI applications and having to train the first line in the peculiarities of these support tools.

Within the results of this research, it has been found that the scope of compliance topics coverage by compliance functions in the case study organizations covers a narrow span.

Based on the definition of this study, compliance per se goes into every aspect of an organization, and not just in areas such as competition, integrity, capital markets, third party due diligence, export/embargo, and anti-bribery (to name just the typical ones identified in this research). A good indication of this fact, originating in the results of this research, is the comprehensive list of resources for assistance, available to employees in one of the case study organizations. This list informs on policies and contact roles regarding compliance and other regulations and standards across the entire enterprise. Confirming the actual enterprise span of compliance management, are further results of this research, indicating the fact that many tools are already enabling the business and operations to be compliant in an autonomous way within the operations units (the first line of defence). These tools are considered policy compliance tools, as they are designed to be compliant (CbD) and therefore enabling the first line of defence to operate in a compliant manner with the support of automation (being augmented in their decision-making process). Such results reveal the fact that AI applications enabling compliance are already in use across business units in organizations, although they are not necessarily regarded as compliance tools. Given the definition of compliance in this research, it can be concluded that automation and AI enabling compliance management is already present to a certain degree within organizations.

When it comes to responsibilities within a CMS, there is no blueprint identified within the results of this research that can be replicated across multiple organizations. Findings show trends towards embedding compliance-specific responsibilities within different business units through the allocation of so-called account managers from the second line of defence functions. These account managers are the source of information on emerging compliance requirements, while the business units hold the responsibility for ensuring adherence to these requirements. This is arguably a good solution to tackle the aim of having compliance activities be part of the culture and lived experience of an organization, by involving stakeholders and making functions and units accountable. Results of this research also show that a great deal of compliance requirements comes from the world of projects, and with an increased push towards innovation and automation, this trend is likely to continue for the years to come. To enable the compliance tasks and responsibilities of both first and second lines of defence in the contexts described above, AI applications can be used to make communication more efficient, and therefore support innovation. Such examples were not seen in the results of this research.

Reporting of compliance-related activities as indicated by the research results, can be seen to be as automated as the activity being reported. In such cases (e.g. cyber security) where a lot of automation exists, reporting is also automated through real-time dashboards and the possibility to put together reports with little human interference. Such reporting is achieved partly due to the fact that the data used by AI applications, can easily and quickly be queried to produce meaningful reports that provide senior management with the information they need to monitor compliance adherence, and ultimately steer the business if necessary. These reports are based partly on auditable data, as indicated by Ramanathan et al. (2007), therefore playing a key role in managing compliance.

2) Enablers and barriers of AI

In defining the type of AI organizations a legal entity can be, literature has identified three types: the data science organization, the machine learning organization, and the hybrid of the two (Workera, n.d.). Positioning this segregation in the context of the findings of this research means looking at what topics must be addressed in order for organizations to be able to have either actionable insights, automate tasks and scale products, or a combination of the two. It is considered to be a strategic decision for organizations to agree on the type of AI entity to invest in, even more so since this decision will be the overarching enabler of AI. Arguably, the data governance and data management maturity of the organization drives this decision. With a mature, data-driven organization, a hybrid type of AI approach can be pursued. Such an organization requires next to a mature data governance, the right IT infrastructure to be able to deploy such applications. The results of this study point out this fact, by drawing the attention to enablers of AI adoption, namely to increased computing capacity (through cloud and edge computing) and increased network capacity (represented by the amount of data traffic that a network can handle at a given time, according to a definition by Arena Com Ltd. (n.d.)). The two themes of data governance and IT infrastructure are highly interconnected in this discussion, because data governance has to answer or at least address the questions on where and how data is stored, processed and visualized (e.g. on-premise, cloud storage, third party providers). Here too, the collaboration with third parties is paramount, as SLAs will be the rule of law against which compliance requirements of one party will be checked to monitor the adherence to defined and accepted specifications of service. Further results of this research show that one of the enablers of AI adoption is the fact that tools are augmenting the capabilities of people. Reducing complexities and eliminating time spent on manual and time-consuming tasks, people can now focus on real business activities. This finding is accentuated by an article from recent years, which focuses on the comparative advantages held by humans and machines when it comes to the characteristics of decision-making (Jarrahi, 2018). If organizations are to take advantage of the capabilities of AI, and use it, among other things, to enable the management of compliance tasks, then strategic decision makers in those organizations have to see "AI as a tool for augmentation (extending human's capabilities) rather than automation (replacing them)" (Jarrahi, 2018). This is the kind of senior management buy-in and support, which the results of this research speak about as enablers of AI adoption within the case study organizations. Among the documentation analysis results of this research (case 2), the attraction of skilled labour in the area of AI and digitalization is a key finding, as indicated by the type of roles the organization is looking to recruit.

Looking at the flip side of how strategic decision makers see AI as a technology, Jarrahi (2018) indicates that, what can be considered a barrier to AI adoption is the fact that leaders in organizations fail to correctly appraise the long-term business value of AI adoption, by focusing on short-term return on investment. Hence, many organizations lack the patience of seeing AI-enablement materialize and deploy it in uncoordinated manners. Although the results of this research cannot accept or deny the above, it is worth taking into account Jarrahi's (2018) indications when it comes to aligning senior management in their decisions on the type of AI organization they want to become.

3) Control and compliance of AI applications

As seen in recent theory, the need of people to understand the process an AI application goes through in coming up with decisions, is increasing, leading to the concept of creating and implementing so-called "Responsible AI" (Barredo Arrieta et al., 2020). An AI application that easily demonstrates responsibility through fairness, explainability and accountability is what stakeholders need to adopt in order to be able to, as seen in the case studies' data, eliminate employees' fear of "putting yourself in the arms of computer programs or algorithms" (interview partner 1, case 3). Furthermore, the fairness, explainability and accountability principles will make it easier for the third line of defence (audit functions) to run its work, and offer assurance on the control and compliance requirements of AI applications. Findings also indicate that in order to maintain control of AI applications, these applications need to be designed in a deterministic way, by eliminating medium-level compliance and striving for one hundred per cent compliance. The findings go on to suggest engineering processes to be redundant in situations where humans are involved, that means eliminating the possibility of a human tampering with results. It is therefore required to embed strong requirements in the CbD principles that guide the development and/or adoption of new AI applications.

4) Compliance by design (CbD)

All case study organizations have confirmed the importance of CbD within applications and processes. Compliance by design is two-folded: (1) CbD within policies and procedures and (2) CbD in new products/services. CbD within policies and CbD within products/services are interconnected as one feeds the other, they need to go hand-in-hand and continuously adapt along the way. The results speak about CbD being a default consideration nowadays, when designing new products and services, with a lot more demand for AI applications coming from the business side. To enable the business side to embed these design-phase compliance requirements, IT and legal departments have become increasingly integrated in business processes rather than being remote support functions (as previously considered). At the same time, in adopting AI applications and ensuring compliance in the design phase, the results speak about the utmost importance of testing of such applications to ensure the quality and compliant behaviour of their output. In this respect, quality and sufficient data is needed to ensure that proper training of the AI models is conducted and then tested for achieving the required results. Hence, CbD considerations need to be a core part of the data governance and data management decisions made by organizations (another theme resulting from the data collected through this research). At the same time Pluta & Poska (2010) mention, that a "periodic review of CbD non-conformances would provide a qualitative and quantitative measurement of system compliance performance", which is in line with the results of this research, indicating that to be compliant by design means to also have means of tracking and monitoring (finding for example exceptions to the designed system and building in rules to deal with special circumstances of those exceptions).

5) Data governance and data management

Findings from this research show that organizations have an increased dependency on data for adopting AI applications, including AI-driven applications that support the organization's CMS. Guidance in literature exists, with researchers and practitioners suggesting data governance models have to manage all the data within an organization, both analytical and transactional data (Slánský, 2018). The organizations interviewed within this research display certain maturity in this field, with the examples of creation of data exchange platforms or sharing data with third parties (both analytical and transactional data). Both these trends are in line with recent literature claims on the organizational scope of data governance being divided into intra- and inter-organizational (Abraham et al., 2019), which means organizations have to establish a governance model to cover internal and external data management requirements.

The European General Data Protection Regulation (GDPR) is probably the most important regulation in Europe, when it comes to data governance aspects, which a CMS in organizations nowadays have to address. In light of the GDPR compliance requirements, organizations have to ensure that the regulation is embedded in their systems and processes. Butterworth (2018) discusses how GDPR requirements pose technical challenges to the development of AI, yet these requirements help bring transparency with regards to data protection designed within AI algorithms: "organisations that are able to anonymise the data they are processing will be in a strong position to protect themselves from complaints relating to their obligations under the GDPR". This observation can be linked to two previously discussed resulting themes of this research: control and compliance of AI applications, and CbD. Tackling the GDPR-related technical challenges in developing AI applications with CbD principles in mind, is a prerequisite in ensuring that control and compliance of those AI applications is achieved, and therefore organizations can reach that position of protecting themselves from complaints. They reach this status by being able to demonstrate with easiness the explainability of the applications operated within their environments; in the case of GDPR, the process of data anonymization and the assurance that outputs are correct given the requirements of the regulation. The data protection topic has been highlighted by all three case studies, emphasizing how dedicated officers occupy central roles in the current respective compliance management processes, to tackle in particular the GDPR.

An effective data governance and data management programme represents at the same time an enabler of AI adoption, making the link to the other prevailing theme from the results of this study (enablers and barriers of AI). The results of this study indicate that a robust data management is needed to unlock AI possibilities by building the foundations on how to manage data, structure it, govern it and leverage it to create applications that enable even a CMS. The governance programme is supposed to bring data together by building a data lake. Findings also make comparisons to other support functions in organizations, such as the finance unit, which is well organized and has well-established processes. By making this comparison, it is noted that such well-established processes are needed when it comes to accessing data as part of the overarching governance of data. This will make the deployment of AI applications a smoother and faster process, while being consistent across the organization. The need for this consistency is accentuated by the fact that data management has a high concern with compliance topics, since complex decisions and rules need to be considered within applications across diverse world jurisdictions, and these applications are all dependent on data. Further criteria in data governance include the need for quality-checked data in order to avoid bias in decisions supported by AI applications.

Going even further, the connection between data governance and data management, and the collaboration with external parties can also be considered an enabler of AI. This is yet another example of how the themes resulting from this study speak to each other, and how they form an ecosystem of AI-enablement towards managing compliance in organizations. The collaboration with third parties has to be oriented towards a common goal, of developing AI applications that are compliant in nature (CbD), and that enable (make it easier and more efficient) all parties involved to do their job. Examples of collaborations with external parties include those with suppliers. In this sphere, the findings of this research briefly touch upon considering the implications of compliance and data security in data sharing and data storage when working with cloud providers. Out of these implications, the compliance of security of data, is a topic that opens up the next theme resulting from this research under a CMS enabled by AI: cyber security.

6) Cyber security

The security of communication and automatic control systems, and ultimately of the information hosted within these systems, is the concern of cyber security (Oxford English Dictionary, n.d.). Srinivas, Das, & Kumar (2019) refer to cyber security as “the protection of internet-connected systems, such as hardware, software as well as data (information) from cyber attacks (adversaries)”. Compliance to cyber security rules covers all three lines of defence, where we have the first line having to comply with so-called information security policies, which are communicated by the second line of defence on the use of information systems (Tsohou & Holtkamp, 2018). Literature indicates that users in the first line of defence require certain competencies according to the communicated policies, yet the professional competence frameworks enacted upon these employees are lacking organizational management knowledge and are not designed to provide control-specific awareness and training programmes (Tsohou & Holtkamp, 2018). The findings within this research, from one of the case studies in particular, are in agreement with the above literature, and emphasize the importance of not only regular training of employees in the first line of defence, but also highlight the need and importance of the monitoring process which is associated with the second line of defence, namely the IT department. The role of the third line of defence in this case, is to offer the assurance over the process, findings indicating the high importance in having qualified, trained individuals offering this assurance. It has also been noted that it is the organization's responsibility to ensure that parties having the required qualifications conduct the assurance offered by the third line of defence. This is partly due to the fact that these internal compliance requirements, of ensuring cyber security, are then subject to external compliance standards (e.g. ISO 27001 or PSI DSS as indicated in the research findings). Only if all three lines of defence can demonstrate to be working as expected in this process, will the certification of compliance to an external standard be achieved. What the results tell us overall, is that there is "a lot of compliance needed to meet certification requirements." (interview partner 2, case 1).

This is another example of how the themes identified within this research speak to each other, in this case "cyber security" practices being driven by the standards enacted by "regulation and regulators". Literature on the topic indicates challenges when it comes to standardization in cyber security, among which are a lack of agility in designing and agreeing on standards, and the existence of competing sets of standards (Srinivas et al., 2019). Despite this, the results of this research point into a slightly different direction, where it is considered that compliance management best practices are currently found in cyber security. Furthermore, since the findings from this research also indicate the fact that cyber security is an area displaying a high maturity in the sphere of AI adoption, it is worth for organizations to consider learning from what has been achieved in cyber security both from an AI-adoption and a compliance management perspective.

7) IT infrastructure (software and hardware)

The theme of IT infrastructure in organizations, referring to both software and hardware, resulted from the data analysed in this research. It was noted how these elements are correlated to the capabilities of the AI applications an organization implements. The discussion is limited to the points brought-up during the data collection phase of this study. The two sub-themes that surfaced as parts of this theme are cloud-computing and service providers. Organizations have indicated how the reliability of their IT systems is a key consideration when it comes to decisions around data storage and processing, and whether or not to use local data servers or a cloud service provider. The availability of operational data is regarded as critical, and as such it poses a high-risk area, making data management and respective compliance paramount. To enable the adoption of AI applications, one of the case study organizations (case 2) has engaged in a partnership with a large global cloud service provider. The key consideration of this partnership rests in allowing the merger of data from various business processes to support the stability of the organization's core operations by managing irregularities. Other considerations around cloud computing, as resulting from this study, include automated security design, automated user provisioning, and security controls. For an organization operating in various world jurisdictions, the quick deployment of these cloud-computing aspects, are decisive. Other studies look at the requirements of successful implementations of cloud-computing and confirm, "specific regulation is required to address the security and privacy of cloud-based services" (Ali & Osmanaj, 2020). The results also indicate that organizations have complex IT architecture landscapes, which can be judged to be posing a lot of different challenges related to compliance management. This complexity is accentuated by having to work with different service providers. Reaching trust in these providers and ensuring compliance according to the defined SLAs, bring more elements to the complexity picture. There are studies suggesting making use of trust evaluation systems that are compliance-based, to support organizations in evaluating cloud service providers based on different criteria (Singh & Sidhu, 2017).

Overall, in the area of IT infrastructure, the latest developments such as increased computing capacity (partly due to cloud-computing availability) and increased network connectivity to organizations represent an enabler for organizations to adopt AI applications. The results of this study suggest that with the growing experience in project implementation of such technology, it is becoming easier for organizations to decide to embed AI applications across the board.

8) Regulation and regulators

Regulation and regulators setting mandatory standards for certain processes or industries (external compliance) often drive the internal compliance requirements and therefore the processes put in place to adhere to these. When it comes to ethics of automation and AI applications, a lot of things don't currently have an answer from a regulatory perspective, with a tremendous amount of research aiming to answer various questions. A recent paper argues that ethical principles have to be transferred into law, and AI needs to be regulated by international law, with established cooperation structures between global, regional and local level norms (Robles Carrillo, 2020). Until maturity in this area is reached, individual organizations and other industry-specific associations are expected to take the reigns in embedding ethical principles within the design of their IT systems and applications. This is seen in the results of this study, where organizations mention that the still-to-be-developed automation compliance frameworks need to integrate considerations on what AI means for the future of work, for the community, for the environment. At the same time, findings show that a lot of things remain currently without an answer and developments in the AI sphere are progressing without necessarily having consensus on the topic. Results suggest that organizations engage in voluntary compliance due to the lack of standards in certain new areas. Nevertheless, there are positive observations that can be made based on the results of this study. These observations show that organizations are partnering up with both regulators and other suppliers, or even competitors, to jointly develop industry standards. At the same time, it has been found that the general relationships with regulators are very important, as these drive the developments on both sides: new regulation and new technology. To accentuate the relationship regulator-organization aspect, as highlighted in the literature review, Parker (2003) sees the communicative energy in the typical compliance program audit as a limiting factor. Therefore, the efforts taken in building new regulation should be complemented in the future by an improved communication and collaboration as part of the third line of defence work (e.g. compliance program audits).

9) Collaboration with external parties

Throughout the previously discussed themes various topics involving a degree of collaboration with external parties were brought up. These topics highlight the interconnectivity between the different aspects of a CMS where AI applications are adopted. When it comes to external parties represented by collaborators or complementary businesses, it has been found within this study, that it is important to implement similar IT systems between the organization and those external parties, in order to ease the process of compliance. The collaboration between such parties goes further to suggest that the parties involved should take part in pilot projects, share lessons learned and therefore together push for faster innovation in adoption of AI applications. Due to existing regulations related to safety and security, the results indicate that in certain type of AI applications' projects, the collaboration goes as far as for the end client to take over the responsibility of collecting the data needed to train the AI application about to be trialled. With this approach, it is ensured that the innovation and development projects are not stalled due to long bureaucratic compliance tasks. Considering the interconnected global world most organizations operate in, such cooperation approaches when it comes to adoption of AI applications and related compliance requirements, makes the case for more seamless implementations and operations.

Findings of this research suggest that considerations regarding system architecture such as where the data and the applications are going to be hosted, user types, countries, all need to be dealt with together with external providers of such products and services. In addition, in order to ensure supplier compliance to agreed-upon terms of business, sound SLA contracts have to be put in place, as well as regular update meetings have to be established. A recurring finding within the data from the case studies of this research is represented by the dependency on legacy system providers (providers of IT systems and services, which have been on the market for a long time, have a large market dominance and therefore very little competition exists), dependency that causes inefficiencies in operations and in the potential adoption of new technology. The replacement of such legacy systems is considered cumbersome, and the establishment of SLAs that meet the requirements of the organizations itself, is posed with feasibility questions. Going back to the theme “IT infrastructure (software and hardware)” cloud-computing was found to be an important sub-theme when it comes to deploying AI applications. The topic of cloud-computing is strongly connected to the theme “collaboration with external parties”. This is the case due to the fact that the adoption of such infrastructure by an organization comes along with the need to align and coordinate a long list of requirements related (but not limited) to data management, security design and controls, user provisioning.

8. Conclusion and limitations

8.1. Conclusion

Beyond anything else, a sound and healthy compliance system is driven by ethical conduct. Within the documentation of the case study number one, it was beautifully written, that "ethical conduct requires more than simply complying with the laws, rules and regulations; good judgement and common sense are crucial." With this in mind, this research draws its conclusions on the conceptual guidelines for an AI-driven CMS that are applicable across an organization, to be led by people with informed judgement and who can use common sense as to what is ethical and what not. Automation/AI is here to inform humans, and not to replace them. It enables people in their day-to-day work and augments their decision-making process, by scaling up the analytics volumes, and allowing the focus to go on more subtle topics, where common sense is required. This common sense is unlikely to be programmed into a line of code; therefore, automation and AI are enablers, and not a replacement of humans, in any area, nor in compliance management. There is a tremendous amount of dependencies that an organization has to take into calculations on the road to becoming an AI-driven organization, and at the same time enabling a system of compliance management across the organization. Whether or not the focus is on actionable insights that enable decisions, or on automating tasks and scaling products and services, all computer systems adopted by an organization should pass the test of being compliant by design (therefore offering control over the compliance of AI), should have access to reliable data through a mature data governance programme, should ensure the security of information and other communication and control systems embedded within, and should be built on a stable and reliable IT infrastructure (software and hardware). Furthermore, the dependencies on external parties need to also be weighted in, as well as the relationship with regulators. The latter can either be an enabler or a barrier, depending on the speed of collaboration, development and accuracy of regulation affecting these AI computer systems. All in all, an obvious outcome of the thematic analysis done within this research is the interconnection between the nine themes resulting from the case study research.

The review of literature demonstrated that the topic of compliance management systems is multifaceted with various categories of subjects on the management of compliance, such as: business processes, audits, compliance information systems, risk-based compliance, corporate compliance systems, governance of AI. The elements of a CMS, as informed by the literature review, have been split using the three lines of defence model, hence guiding the dynamics of tasks and responsibilities across an enterprise.

The analysis of the set-up and design of CMSs in organizations, using the CMS ecosystem framework produced by the literature review phase, has resulted in a number of propositions that cover both strengths and weaknesses of the design of a CMS in the case study organizations. The results of this analysis suggest that organizations delegate formal compliance tasks to a compliance function, covering key compliance areas, while at the same time a large number of compliance activities belong to other functions, and are not necessarily captured within the official CMS of that organization. In addition, the degree of maturity of AI adoption, and even more so, AI adoption in compliance management, is not very high. This suggests a weakness in the set-up of CMSs in organizations, with enterprises at a stage of focus on pilot projects and experimentation with AI solutions. The exploration on how AI can strategically demonstrate being an enabler of compliance management activities has resulted in key themes that organizations ought to consider in the pursuit of using AI applications. These themes address first of all the general components, structure and responsibilities in a CMS, then move on to cover enablers and barriers of AI adoption, control and compliance of AI applications, compliance by design considerations, data governance and management, cyber security, IT infrastructure, regulation and regulators, as well as collaboration with external parties. Possible interpretations of these themes include the fact that the comprehension of the connectivity among them can lead organizations to tap on the potential of using AI applications across the board, augmenting people in being compliant and managing compliance requirements with a smarter use of resources.

The contribution to knowledge and practice of this research lies in the understanding of how compliance management systems are set-up in organizations, by using the CMS framework derived from literature, later confirmed by empirical data. Furthermore, this research contributes to both knowledge and practice, through the depiction of the enablers and barriers of AI adoption in organizations, as well as the recommended conceptual guidelines for AI-driven CMSs (to follow in the next chapter). This contribution is here to inform senior management and executives in large organisations, on key considerations to make in adopting AI. Most importantly it informs these individuals how AI can be deployed across an organization with the aim of supporting the enterprise to perform its compliance management duties and tasks.

8.2. Limitations

This study is not without its limitations. First, empirical data were obtained from three case studies belonging to one overarching industry. These organizations were selected based on the criterion of being large organizations. Likewise, conclusions and recommendations are derived from these three organizations. Accordingly, findings cannot be generalized and must be treated with due attention, while the applicability of the findings to other organization sizes or other industries may be limited. Future research should be done with more data collected from organizations from multiple industries.

Secondly, interview partners were selected based on the specified requested list of roles, and the acceptance depended on the snowballing sampling technique. As such, the observations made from this empirical data can be considered biased by the function and department to which these interview participants belong. Hence, future research should expand the span of functions interviewed, and even go to the board of directors' level.

Thirdly, the focus of the research questions used in the data collection phase has been a strategic one and as such kept a distance from details on implemented automation/AI applications. Future research could shed light onto the particularities of the computer system applications that enable staff to perform their compliance management duties.

When it comes to the timeframe of the research, this study used a cross-sectional approach. A longitudinal study could in fact bring up more data that relates to the culture of compliance management in organizations.

The retroductive explanation of this research should ideally be tested with respondents from where it has been derived. Subsequent variation through discussion can then be put forward for researchers to question and test in alternative contexts. For testing to be effective, the process of testing would have to be very extensive and conducted over a considerable period of time. This type of research would be dependent on time constraints as well as respondents' commitment and represents therefore an area for future research.

A study that would make sufficient specific observations would have to be conducted through subsequent ethnographic experiences within different business units of an organization, allowing for complete observations of the studied phenomena (the system of compliance management within the organization), and for the chance to be part of the intangible aspects of a system of compliance management. Such a research would likely lead to specific observations and therefore would be capable of drawing a general conclusion. An ethnographic research would also be able to understand and explain the causal powers in the second level of the stratified reality introduced by Roy Bhaskar (Benton & Craib, 2011): the ‘actual’ sequence of events, which occur outside the laboratory, but are rather encountered in lived conjunctures. An example of an ethnographic research within a compliance unit of an organization was mentioned earlier in the literature review (Pérezts & Picard, 2015), however this example was limited to one business unit only, therefore not covering the enterprise view on compliance management.

9. Recommendations and implications

After investigating and analysing how compliance management systems (CMSs) are strategically set-up in organizations, listing the enablers and barriers of AI adoption and touching upon the way CMSs are supported by AI applications, this study presents here its final recommendations. The results and findings have led to the previous discussion and conclusion, based on which this research is now able to provide recommended conceptual guidelines on deploying enterprise-wide compliance management systems enabled by AI. This research reveals the conceptual guidelines, which are grounded in the context of the case study organizations and at the same time relevant due to their theoretical underpinning. These guidelines are recommendations to organizations. Some would argue that the guidelines should have been more specific to the compliance function or that the research is too generic. Yet, this study managed to meet its aim through fulfilling its five objectives, and has therefore resulted in twenty-four actionable guidelines by practitioners. This chapter is composed of two parts: (1) conceptual guidelines for AI-driven Enterprise Compliance Management Systems, and (2) implications for future research.

9.1. Conceptual guidelines for AI-driven Enterprise Compliance Management Systems

The recommendations of this research are two-fold: on the one hand they draw the attention to the need to carefully consider the enablers and barriers to AI adoption within organizations, and then propose a list of twenty-four conceptual actionable guidelines to senior management of large organizations, on what they should consider when aiming to deploy an AI-driven CMS. These conceptual guidelines are then allocated (presented in a tabular form) to the respective line of defence, as well as to the board level (which ultimately should enact the recommended guidelines).

The initial recommendation is to first of all understand and carefully consider the enablers and barriers to AI adoption in organizations:

- According to the results and discussion of this research, the enabling factors of AI adoption are: senior management support, sound long-term appraisal of the business value brought by AI and as such deciding on the type of AI-organization to pursue; reorientation of employee focus on business activities requiring human judgement rather than manual input, by augmenting human capabilities in complex data-intensive tasks; reduction of costs; strong data management practice; regulation for new technology driving industry standards and therefore adoption of AI; simplification of internal processes by allowing people to make decisions informed by reliable AI applications; employing adaptable AI applications with data interpretation capability and capacity; economies of scale to invest in AI implementation projects in large organizations; expected improvements in the quality of products, services and customer experience; reduction of staff numbers; new infrastructure developments such as increased computing capacity and increased network connectivity; positive results from AI pilot projects; legal, safety and security requirements driving early adoption; cross-industry collaboration and sharing of lessons learned; easiness and reduced costs of implementation of AI applications.

- The factors regarded as barriers to AI adoption are: illiteracy of senior management when it comes to what AI is and is not; the lack of understanding of business processes and dependencies amongst these processes; a weak or inexistent data management practice within organizations; heterogeneous IT application landscapes in organizations; high costs related to implementation projects; inexistent regulation for new technology; high level of due diligence on suppliers and respective infrastructure offered; large number of stakeholders increasing the amount of compliance requirements to be met and also delaying the decision-making process making certain AI applications obsolete; monopolistic distribution channels for products or services; changes in liability and legal requirements that come along with AI adoption; resistance to change by employees; stakeholders' fear of ending up in the control of computer programs or algorithms; safety and security requirements putting hurdles to innovation and delaying implementation projects.

Secondly, the conceptual guidelines for the set-up of an enterprise-wide compliance management system driven by AI are depicted from the point of view of helping organizations overcome the barriers of AI adoption and allowing them to tap on the enablers of it instead (as resulting from this research). The following twenty-four guidelines are therefore the second part of the recommendations of this research, literally expressed here for guiding senior executives and board members alike (boards of management, boards of directors), on their path in supporting their organizations in their compliance management endeavours, by adopting AI applications. Therefore, it is recommended for the senior management and board of directors of organizations to understand, enact and action upon the following guiding lines:

1. The goal of a CMS should be to have an organization-wide set of detailed methods, procedures, and routines that support the company to manage the business processes and applications' adherence to internal and external requirements that emerge from different sources. This set of detailed methods, procedures and routines should cover the entire spectrum of the organization (exist and be lived at an enterprise level by being carefully allocated to the three lines of defence). Therefore, a set of AI applications' solutions for compliance management based on the three lines of defence of an organization should be created: core business units, support and oversight functions, and audit functions. In parallel to this endeavour, consult and follow the "ISO 19600:2014 Compliance management systems guidelines" (International Organization for Standardization, 2014).
2. Understand or agree on the strategy of the organization when it comes to the type of AI organization the company is: data science, machine learning or a hybrid organization. The type of AI governance considerations to be given to these types of organizations differs, therefore it is important for organizations to have a clear strategy regarding their ambitions with AI. This will also have an impact on the building blocks of AI suggested by a HFS Research study (Fleming, 2019), that are adopted across the enterprise and will allow the understanding of which of these AI blocks can enable the compliance management processes. The blocks are: fundamental AI (machine learning, deep learning), focused AI (natural language processing, computer vision) and packaged AI (autonomics, cognitive agents, digital twins) (Fleming, 2019).
3. Have full senior management support in implementing the AI strategy of the organization.
4. Clearly allocate responsibilities during the change process (e.g. quality assurance of the underlying algorithm of the AI application, execution and output of the AI application) when adopting AI applications (computer systems that augment the activities of emergence and adherence to internal and external requirements such as laws, legislation, regulations, standards and/or codes of practice).
5. Develop a long-term strategy for data governance and data management, and start by classifying data according to criteria: forms of data (structured and unstructured), types of data (transaction, master, and reference), uses of data (operational and analytical), origin of data (internal and external) and data stability (short-term perishable/volatile and long-term static and slow) (Slánský, 2018).

6. Ensure sufficient, reliable, unbiased and fair data is available for testing.
7. Ensure data sharing and security requirements are defined when engaging with third parties (e.g. part of the GDPR compliance management).
8. Make use of the maturity of AI adoption with regards to compliance management in cyber security. Start by aligning experts in the organization and understand what has been achieved so far, tapping on the best practices of deploying AI in securing the organization from cyber-attacks.
9. Design policies, procedures, manuals and set-up requirements for new AI applications by embedding the principle of "Compliance by Design" from the beginning. In doing so, involve all stakeholders in the development and change process.
10. Design new AI applications using a user-centric approach to make it easier for employees and other parties to be compliant, rather than non-compliant.
11. Recognized compliance patterns that are translated into formal compliance rules within company-wide compliance management applications, should be supplemented by employee actions that work complementary, forming an all-dimension compliance management system. Compliance behaviour is mediated by compliance knowledge because it fosters voluntary compliance, therefore training on the organization's policies and procedures should be constantly offered to employees and other stakeholders.
12. Offer training to employees, on the basic functionalities of AI applications, thus eliminating the fear of ending up in the control of unknown computer programs or algorithms, and the associated resistance to change.
13. Build AI applications that have reliable, simple and comprehensive fall-back steps, and design processes that are redundant to people interacting with it.
14. Ensure maturity of the third line of defence when it comes to skills for auditing AI applications, through specialized training and/or using third party auditors.
15. Consider the type and form of audit logs produced by the organization's IT systems, which help demonstrate the enforcement of compliance in an organization's IT infrastructure (including IT controls that meet IT compliance objectives).
16. Ensure control over AI applications; this means understanding what compliance requirements have been designed and embedded within the applications themselves. The data used by these applications represent the fuel on which they run and it needs to be ensured these data exhibit fairness, allow for model explainability and accountability.

17. Interlink “data governance and data management” considerations, “Compliance by Design” requirements and “control and compliance of AI applications” standards. These three areas ideally work hand in hand since they depend on each other.
18. Set-up collaboration platforms with external parties and other industry players to share best practices in deploying AI applications, compliance requirements, and to help shape future regulations.
19. Consider the interdependencies between internal and external compliance requirements. Regulation and regulators setting mandatory standards for certain processes or industries (external compliance) often drive the internal compliance requirements and therefore the subsequent processes put in place to adhere to these.
20. Work together with regulators from an early phase to quickly enact industry standards for AI applications, which in turn will drive a higher and sooner adoption of such applications.
21. Invest in AI pilot projects to demonstrate the benefits of using AI on e.g. the quality of products, services, customer experience, employee well-being, and therefore get the buy-in of stakeholders.
22. Consider harnessing technology to gain a uniform view of information available and to organize risk management efforts. With the support of a Governance Risk and Compliance (GRC) IT system designed to meet the needs of all three lines of defence, an enterprise-wide CMS can be enabled since the governance aspect of compliance management, the risks and the responses to it are embedded in applications that speak the same language, of one GRC system.
23. To harness technology, set-up an infrastructure supportive of the AI applications by investing in both hardware and software and tapping on the increased computing capacity as well as on the increased network capacity and connectivity.
24. Invest in a capable, technology-driven legal team, and set-up requirements for thorough due diligence processes when adopting AI applications.

The guidelines resulting from this research have been allocated to the three lines of defence model of an organization: first, second and third lines, plus the board of directors. The board of directors represents the overarching power steering the way in which the lines respond to risks and opportunities to protect the organization and help it achieve its objectives. Given this role, this research allocates its recommendations based on the three lines of defence model to include also the oversight role of the board of directors in this framework. This allocation indicates to which line or level of the organization the respective guideline(s) are addressed.

By addressing these guidelines, it is expected that accountability and responsibility be assumed, to act upon the guideline(s). Therefore, the table below (Table 3) is a two-level matrix that on the horizontal line indicates the above-mentioned allocation, while on the vertical line indicates the key theme resulting from this research, to which the guidelines are linked. The "#" in the table represents the actual number of the resulting twenty-four conceptual guidelines, as allocated above. Some of the numbers (e.g. #11 (involvement)) have a parenthesis that is indicating the fact that for that particular guideline, the line of defence or the board of directors has a particular responsibility with respect to acting upon the guideline.

Table 3. Recommended guidelines based on a two-level matrix: AI-enabled CMS themes, organizational defence lines and compliance

Organizational defence lines and compliance levels **AI-enabled CMS themes**	**First line of defence**	**Second line of defence**	**Third line of defence**	**Board of Directors level**
1) CMS components, structure, responsibilities	#4 #11 (involvement)	#4 #11	#4 #14 #22	1# #14 #22
2) Enablers and barriers of AI	#4 #8 (involvement)	#3 #4 #8 #21 #24	#4	#2 #3

3) Control and compliance of AI applications	#16 (operations)	#12 #13 #15 #17	#14 #15 #16 (assurance)	#14 #17
4) Compliance by Design		#9 #10 #13 #17		#17
5) Data governance and data management	#16 (operations)	#5 #6 #7 #17	#16 (assurance)	#5 #17
6) Cyber security		#7 #8		
7) IT infrastructure (software and hardware)		#23	#22	#22 #23 (strategic)

8) Regulation and regulators		#19 #20 #24	#20 (involvement)	
9) Collaboration with external parties	#18 (involvement)	#7 #18		

9.2. Implications for future research

Based on the outcome of this research, it is proposed in this section the three core subject areas that future research should address. These areas are:

1. Expanding the research of tackling AI within IT governance (as part of corporate governance). Given the position of the control and compliance of AI within the IT governance responsibilities of an organization, it is worth to conduct further research to support organizations structure the adoption of AI in a mature way.
2. Studying the impact of COSO and the role of ERM to support risk management and internal control mechanisms in the wake of AI developments. With AI, many unknowns are on the horizon, in particular within an organization's processes. Risk management and internal controls across an enterprise will have to respond and keep pace with this changing behaviour in processes and ways of working. Therefore, this is an area for potential future research.
3. Studying the role of external regulators with regards to deploying and regulating AI together with the board of directors. Results of this study have indicated the importance of collaborating with external regulators from early stages when it comes to AI adoption. There is an obvious need for expanding the research in this area, to bring up innovative ways of collaborating with the regulators, fast enough, responsibly and sustainably.

Future research could also explore user-oriented methodological approaches to rethink the enterprise system of compliance management in organizations, which could potentially help companies implement the conceptual guidelines resulting from this study, by adopting a user centric approach. Overall, the guidelines resulting from this study are meant to be of a strategic importance, and to address the initial research problem from a conceptual point of view.

References

Abdullah, N. S., Indulska, M., & Sadiq, S. (2016). Compliance management ontology – a shared conceptualization for research and practice in compliance management. *Information Systems Frontiers*, *18*(5), 995–1020. https://doi.org/10.1007/s10796-016-9631-4

Abraham, R., Schneider, J., & vom Brocke, J. (2019). Data governance: A conceptual framework, structured review, and research agenda. *International Journal of Information Management*, *49*(January), 424–438. https://doi.org/10.1016/j.ijinfomgt.2019.07.008

Airport Technology. (2019). British Airways trials AI at Heathrow T5 to minimise delays. Retrieved from https://www.airport-technology.com/news/british-airways-ai-heathrow-t5/

Ali, O., & Osmanaj, V. (2020). The role of government regulations in the adoption of cloud computing: A case study of local government. *Computer Law and Security Review*, *36*. https://doi.org/10.1016/j.clsr.2020.105396

Anderson, D. J., & Eubanks, G. (2015). *Leveraging COSO across the three lines of defense. The Internal auditor*. Retrieved from https://www.coso.org/Documents/COSO-2015-3LOD.pdf

Arena Com Ltd. (n.d.). Network capacity - definition. Retrieved from https://www.gsmarena.com/glossary.php3?term=network-capacity

Arndorfer, I., & Minto, A. (2015). *The "four lines of defence model" for financial institutions. Taking the three-lines-of-defence model further to reflect specific governance features of regulated financial institutions* (No. 11). Retrieved from http://www.bis.org/fsi/fsipapers11.pdf

Atkinson, J. (2002). Four steps to analyse data from a case study method. *Association for Information Systems*, *38*(1), 1–11.

Bamberger, K. A. (2010). Technologies of compliance: Risk and regulation in a digital age. *Texas Law Review*, *88*(4), 669–739. https://doi.org/10.2139/ssrn.1463727

Barredo Arrieta, A., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., … Herrera, F. (2020). Explainable Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion*, *58*(December 2019), 82–115. https://doi.org/10.1016/j.inffus.2019.12.012

Basel-Stadt, H. des K. Swiss International Airlines (2020). Retrieved from https://bs.chregister.ch/cr-portal/auszug/auszug.xhtml;jsessionid=42f77abac013f1c5894b02c95bf0?uid=CHE-105.918.070&amt=BS&loeschung=

Belfrage, C., & Hauf, F. (2017). The Gentle Art of Retroduction: Critical Realism, Cultural Political Economy and Critical Grounded Theory. *Organization Studies*, *38*(2), 251–271. https://doi.org/10.1177/0170840616663239

Benton, T., & Craib, I. (2011). Critical Realism and the Social Sciences. *Philosophy of Social Science*, 120–141.

Bhaskar, R. (1978). A realist theory of science. *Hemel Hempstead: Harvester Press.*

Bhaskar, R. (1986). *Scientific Realism and Human Emancipation*. Thetford, Norfolk: The Thetford Press.

Boland, R. F. (2006). Reduce business risk with a CMS. *Chemical Engineering Progress*, *102*(10), 39–44.

Bray, M. (2015). Paul K Edwards, Joe O'Mahoney and Steve Vincent (eds) Studying Organizations using Critical Realism: A Practical Guide. *Journal of Industrial Relations*, *57*(1), 115–118. https://doi.org/10.1177/0022185614560090

Bringsjord, S., & Govindarajulu, N. S. (2018). Artificial Intelligence. Retrieved October 1, 2018, from https://plato.stanford.edu/entries/artificial-intelligence/#HistAI

Butler, T., & McGovern, D. (2012). A conceptual model and IS framework for the design and adoption of environmental compliance management systems: For special issue on governance, risk and compliance in IS. *Information Systems Frontiers*, *14*(2), 221–235. https://doi.org/10.1007/s10796-009-9197-5

Butterworth, M. (2018). The ICO and artificial intelligence: The role of fairness in the GDPR framework. *Computer Law and Security Review*, *34*(2), 257–268. https://doi.org/10.1016/j.clsr.2018.01.004

Cambridge University Press. (n.d.-a). compliance. Retrieved from https://dictionary.cambridge.org/de/worterbuch/englisch/compliance

Cambridge University Press. (n.d.-b). comply. Retrieved from https://dictionary.cambridge.org/de/worterbuch/englisch/comply

Chartered Institute of Internal Auditors. (2019). Governance of risk: Three lines of defence. Retrieved from https://www.iia.org.uk/resources/audit-committees/governance-of-risk-three-lines-of-defence/

COSO. (2017). Enterprise Risk Management Integrating with strategy and performance - Executive Summary. *The Committee of Sponsoring Organizations of the Treadway Commission*, (June), 16. Retrieved from https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf

COSO. (2020). About Us. Retrieved from https://www.coso.org/Pages/aboutus.aspx

Crafts, N. (2006). Regulation and productivity performance. *Oxford Review of Economic Policy*, *22*(2), 186–202. https://doi.org/10.1093/oxrep/grj012

Deloitte. (2017). *Building world-class ethics and compliance programs*. Retrieved from https://www2.deloitte.com/ch/en/pages/risk/articles/building-world-class-ethics-and-compliance-programs.html

Deloitte. (2020). *The future of regulation: Navigating the intersection of regulation, innovation, and society*. Retrieved from https://www2.deloitte.com/ch/en/pages/public-sector/articles/future-of-regulation.html

Deutsche Lufthansa. (2019). *Annual Report 2018*. Retrieved from https://www.lufthansagroup.com/en/themes/annual-report-2018.html

Deutsche Lufthansa. (2020). More stability and reliability for Lufthansa Group customers. Retrieved from https://newsroom.lufthansagroup.com/english/newsroom/all/more-stability-and-reliability-for-lufthansa-group-customers/s/e079f94c-9d1b-44cd-9eae-79d9918cbbaf

Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., … Williams, M. D. (2019). Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, (July). https://doi.org/10.1016/j.ijinfomgt.2019.08.002

Edwards, P. K., O'Mahoney, J., & Vincent, S. (2014). *Studying Organizations Using Critical Realism: A Practical Guide*. Oxford Scholarship Online.

https://doi.org/10.1093/acprof:oso/9780199665525.001.0001

Eisenhardt, K. M. (1989). Building Theories from Case Study Research. *Academy of Management Review*, *14*(4), 532–550. https://doi.org/10.5465/AMR.1989.4308385

Elgammal, A., Turetken, O., van den Heuvel, W. J., & Papazoglou, M. (2016). Formalizing and appling compliance patterns for business process compliance. *Software and Systems Modeling*, *15*(1), 119–146. https://doi.org/10.1007/s10270-014-0395-3

Eurostat. (n.d.). Small and Medium-sized Enterprises (SMES). Retrieved from https://ec.europa.eu/eurostat/web/structural-business-statistics/structural-business-statistics/sme

Farrow, E. (2019). To augment human capacity—Artificial intelligence evolution through causal layered analysis. *Futures*, *108*(February), 61–71. https://doi.org/10.1016/j.futures.2019.02.022

Fleetwood, S., & Ackroyd, S. (2004). *Critical realist applications in organization and management studies*. London: Routledge.

Fleming, R. (2019). Google AI Services Top 10 Report – Excerpt for KPMG, (April).

Fletcher, A. J. (2017). Applying critical realism in qualitative research: methodology meets method. *International Journal of Social Research Methodology*, *20*(2), 181–194. https://doi.org/10.1080/13645579.2016.1144401

Gabbi, G., Musile Tanzi, P., & Nadotti, L. (2011). Firm size and compliance costs asymmetries in the investment services. *Journal of Financial Regulation and Compliance*, *19*(1), 58–74. https://doi.org/10.1108/13581981111106176

Gibbs, G. R. (2013). *Analyzing qualitative data*. Los Angeles: Sage Publications.

Gozman, D., & Currie, W. (2014). The role of rules-based compliance systems in the new EU regulatory landscape: Perspectives of institutional change. *Journal of Enterprise Information Management*, *27*(6), 817–830. https://doi.org/10.1108/JEIM-05-2013-0023

Haynes, A. (2005). The effective articulation of risk-based compliance in banks. *Journal of Banking Regulation*, *6*(2), 146–162.

Heathrow Airport Limited. (n.d.). Who does what. Retrieved from https://www.heathrow.com/company/about-heathrow/company-information/who-does-what

Heathrow Airport Limited. (2019). *Investor Report December 2019*. Retrieved from https://www.heathrow.com/content/dam/heathrow/web/common/documents/company/investor/reports-and-presentations/investor-reports/December_2019_Heathrow_SP_investor_report.pdf

Heathrow Airport Limited. (2020). *Results for the year ended 31st December 2019*. Retrieved from https://www.heathrow.com/company/investor-centre/reports/financial-results

Horne, J. R. (2016). The Nine Critical Questions Managers Should Ask – A Proposal for Evaluating Organizational Efficiency. *NOVA Southeastern University*, *11*(1), 20–32.

IATA. (n.d.-a). Airline Services. Retrieved from https://www.iata.org/en/services/finance/airlines/

IATA. (n.d.-b). Vision and Mission. Retrieved from https://www.iata.org/en/about/mission/

IATA. (2019). Press Release No.74 Management Developments. Retrieved from https://www.iata.org/en/pressroom/pr/2019-12-17-01/

International Organization for Standardization. (2014). ISO 19600:2014 Compliance management systems — Guidelines, *2014*.

ISACA. (2021). History. Retrieved from https://www.isaca.org/why-isaca/about-us/history

Jarrahi, M. H. (2018). Artificial intelligence and the future of work: Human-AI symbiosis in organizational decision making. *Business Horizons*, *61*(4), 577–586. https://doi.org/10.1016/j.bushor.2018.03.007

Kharbili, M. El, Stein, S., Markovic, I., & Pulvermüller, E. (2008). Towards {Policy-Powered} Semantic Enterprise Compliance Management. Discussion Paper. *3rd International Workshop on Semantic Business Process Management {(SBPM)}*, *412*, 16–21.

Kim, S. S., & Kim, Y. J. (2017). The effect of compliance knowledge and compliance support systems on information security compliance behavior. *Journal of Knowledge Management*, *21*(4), 986–1010. https://doi.org/10.1108/JKM-08-2016-0353

Knuplesch, D., Reichert, M., & Kumar, A. (2017). A framework for visually monitoring business process compliance. *Information Systems*, *64*, 381–409. https://doi.org/10.1016/j.is.2016.10.006

KPMG LLP. (2016). 2016 Compliance Transformation Survey, (November).

KPMG LLP. (2017). Compliance Transformation Internal Audit Point of View, (April).

Kumar, V., Pollanen, R., & Maheshwari, B. (2008). Challenges in enhancing enterprise resource planning systems for compliance with Sarbanes-Oxley Act and analogous Canadian legislation. *Management Research News*, *31*(10), 758–773. https://doi.org/10.1108/01409170810908516

Langevoort, D. C. (2002). A firm wants its employees to be sensitive to legal requirements in order to minimize the threat of legal sanctions and reputational harm that it faces when a violation occurs., (c), 1–30.

Lux, A., Hess, J., & Herterich, R. (2013). Business process management as basis for enterprise management systems. *Proceedings - 2013 IEEE International Conference on Business Informatics, IEEE CBI 2013*, 350–355. https://doi.org/10.1109/CBI.2013.57

Müller, S., & Supatgiat, C. (2007). A quantitative optimization model for dynamic risk-based compliance management. *IBM Journal of Research and Development*, *51*(3–4), 295–307. https://doi.org/10.1147/rd.513.0295

Murphy, J. E. (2007). What Is This Field of Compliance and Ethics? *Journal of Health Care Compliance*, *9*(5), 27-32,71-72. Retrieved from http://search.proquest.com/docview/227909665?accountid=14549%5Cnhttp://hl5yy6xn2p.search.serialssolutions.com/?genre=article&sid=ProQ:&atitle=What+Is+This+Field+of+Compliance+and+Ethics?&title=Journal+of+Health+Care+Compliance&issn=15208303&date=2007-09-0

Ng, A. (2019). AI for everyone. Coursera. Retrieved from https://www.coursera.org/lecture/ai-for-everyone/week-1-introduction-SRwLN

Nso, M. A. (2019). Defining Compliance Metric for Management Appraisal, *12*(4), 8–11.

Oliver, C. (2011). Critical realist grounded theory : A new approach for social work research. *British Journal of Social Work*, *42*(2), 371–387. https://doi.org/10.1093/bjsw/bcr064

Oxford English Dictionary. (n.d.). cybernetics, n. Retrieved from https://www.oed.com/view/Entry/46486?redirectedFrom=cybernetics#eid

Padmanabhan, G. (2012). Issues in IT governance. In *BIS central bankers' speeches* (pp. 1–8).

Papazafeiropoulou, A., & Spanaki, K. (2016). Understanding governance, risk and compliance information systems (GRC IS): The experts view. *Information Systems Frontiers*, *18*(6), 1251–1263. https://doi.org/10.1007/s10796-015-9572-3

Parker, C. (2003). Regulator-required corporate compliance program audits. *Law and Policy*, *25*(3), 221–244. https://doi.org/10.1111/j.1467-9930.2003.00149.x

Parker, C., & Nielsen, V. L. (2009). Corporate Compliance Systems. *Administration & Society*, *41*(1), 3–37. https://doi.org/10.1177/0095399708328869

Pawłowski, M., Piatkowski, Z., & Żebrowski, W. (2009). Management Efficiency. *Foundations of Management*, *1*(1), 95–110. https://doi.org/10.2478/v10238-012-0007-x

Pérezts, M., & Picard, S. (2015). Compliance or Comfort Zone? The Work of Embedded Ethics in Performing Regulation. *Journal of Business Ethics*, *131*(4), 833–852. https://doi.org/10.1007/s10551-014-2154-3

Pluta, P. L., & Poska, R. (2010). Compliance by Design* (CbD) and Compliance Master Plan (CMP)-An Organized Approach to Compliance. *Journal of GXP Compliance*, *14*(2), 73. Retrieved from http://search.proquest.com/docview/501928510?accountid=8144%255Cnhttp://sfx.aub.aau.dk/sfxaub?url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&genre=article&sid=ProQ:ProQ%253Apqrl&atitle=Compliance+by+Design*+%2528CbD%2529+and+Compliance+Maste

Prowse, S. (1994). Corporate governance in an international perspective: a survey of corporate control mechanisms among large firms in the United States, the United Kingdom, Japan and Germany. *BIS Economic Papers*.

Ramanathan, J., Cohen, R. J., Plassmann, E., & Ramamoorthy, K. (2007). Role of an auditing and reporting service in compliance management. *IBM Systems Journal*, *46*(2), 305–318. https://doi.org/10.1147/sj.462.0305

Robles Carrillo, M. (2020). Artificial intelligence: From ethics to law. *Telecommunications Policy*, (April 2019), 1–16. https://doi.org/10.1016/j.telpol.2020.101937

Robotics and automation. (2019). Automation in action at Heathrow Airport. Retrieved from https://www.roboticsandautomation.co.uk/conference-2019/automation-in-action-at-heathrow-airport

Russell, S. J., Norvig, P., & Davis, E. (2010). *Artificial intelligence: a modern approach* (3rd ed.). Upper Saddle River, NJ: Prentice Hall.

Sadiq, S., Governatori, G., & Namiri, K. (2007). Modeling Control Objectives for Business Process Compliance. *Business Process Management*, 149–164. https://doi.org/10.1007/978-3-540-75183-0_12

Sammer, J. (2005). New Horizons: Enterprise-Wide Compliance.

Saunders, M., Lewis, P., & Thornhill, A. (2009). Research Methods for Business Students. New York: Pearson.

Seidl, D., Sanderson, P., & Roberts, J. (2009). *Applying" comply-or-explain": Conformance with Codes of Corporate Governance in the UK and Germany* (No. 389). *Centre for Business Research, University of Cambridge*.

Sesen, M. B., Suresh, P., Banares-Alcantara, R., & Venkatasubramanian, V. (2010). An ontological framework for automated regulatory compliance in pharmaceutical manufacturing. *Computers and Chemical Engineering*, *34*(7), 1155–1169. https://doi.org/10.1016/j.compchemeng.2009.09.004

Sheedy, E., Zhang, L., & Tam, K. C. H. (2019). Incentives and culture in risk compliance. *Journal of Banking and Finance*, *107*. https://doi.org/10.1016/j.jbankfin.2019.105611

Shleifer, A. (2005). Understanding Regulation. *European Financial Management*, *11*(4), 439–451. https://doi.org/10.1080/09528822.2014.970769

Singh, S., & Sidhu, J. (2017). Compliance-based Multi-dimensional Trust Evaluation System for determining trustworthiness of Cloud Service Providers. *Future Generation Computer Systems*, *67*, 109–132. https://doi.org/10.1016/j.future.2016.07.013

Slánský, D. (2018). *Data and analytics for the 21st century: Architecture and governance*. Prague: Professional Publishing.

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, *92*, 178–188. https://doi.org/10.1016/j.future.2018.09.063

Sturm, M. E. (2016). *Corporate Governance in the EU and U.S.: Comply-or-Explain Versus Rule (European Union Law Working Papers)* (No. 16). Stanford - Vienna.

Tadewald, J. (2014). GRC Integration: A Conceptual Foundation Model for Success, *15*(3), 10–19.

Taylor, S. P. (2018). Critical Realism vs Social Constructionism & Social Constructivism: Application to a Social Housing Research Study. *International Journal of Sciences: Basic and Applied Research*, *37*(2), 216–222. Retrieved from http://insight.cumbria.ac.uk/id/eprint/3596/%0Ahttp://insight.cumbria.ac.uk/id/eprint/3596/1/8701-25730-1-PB.pdf

The Institute of Internal Auditors. (2013). The three Lines of Defense in effective Risk Management and Control. *IIA Position Paper*, (January). https://doi.org/10.1039/c1cc12161h

The Institute of Internal Auditors. (2020). About The IIA. Retrieved from https://na.theiia.org/about-us/Pages/About-The-Institute-of-Internal-Auditors.aspx

Tsohou, A., & Holtkamp, P. (2018). Are users competent to comply with information security policies? An analysis of professional competence models. *Information Technology and People*, *31*(5), 1047–1068. https://doi.org/10.1108/ITP-02-2017-0052

Volonino, L., Gessner, G. H., & Kermis, G. F. (2004). Holistic Compliance with Sarbanes-Oxley. *Communications of the Association for Information Systems*, *14*, 1.

Weill, P., & Ross, J. W. (2004). IT Governance. In *Competing in the Information Age: Align in the Sand: Second Edition*. https://doi.org/10.1093/0195159535.003.0008

Willging, P. R. . (2014). Corporate Compliance Isn't Just 'More Government. *The Hispanic Outlook in Higher Education*, *24*(10), 10–11. https://doi.org/http://dx.doi.org/10.1177/1054773811422123

Workera. (n.d.). *The AI Human Capital Playbook*. Retrieved from http://www.bibalan.com/wp-content/uploads/workera.ai-ai-team.pdf

Wright, S. A., & Schultz, A. E. (2018). The rising tide of artificial intelligence and business automation: Developing an ethical framework. *Business Horizons*, *61*(6), 823–832. https://doi.org/10.1016/j.bushor.2018.07.001

Yandle, B., & Young, E. (1986). Regulating the Function, Not the Industry, *51*(1), 59–70.

Yin, R. K. (1994). *Case Study Research Design and Methods: Applied Social Research and Methods Series* (2nd ed.). Thousand Oaks, CA: Sage Publications Inc.

Appendices

Appendix A – categories, codes and definitions

Category	Question types	Sub-questions/themes	Specific code	Definition
A	**General introductory**	AI / automation in operations or trial	A0	Examples of automation or AI applications/tools that the organization currently has in production (operational) or finds itself in a trial-phase (regardless of the area/department/function).
		Strategy for AI solutions	A1	The general/overall strategy of the organization when it comes to automation/AI solutions.
		Strategy for AI for compliance management	A2	The strategy of the organization when it comes to automation/AI solutions to support the management of compliance / activities of compliance management.
		Maturity of AI	A3	The level of perceived maturity of the organization's automation/AI solutions.
		Enablers of AI	A4	The factors/topics that are enabling the organization to adopt automation/AI technology across the board.
		Barriers of AI	A5	The factors/topics that are stopping/blocking the organization to adopt automation/AI technology across the board.
		Organizational structure	A6	The structure of the organization: departments, units, etc.
		Compliance function structure	A6-1	The structure of the compliance department/function (e.g. position within the organization, reporting lines etc.)
		Formal CMS existence	A6-11	Information on the existence of a formally named "Compliance Management System (CMS)".
		Responsibilities	A6-12	The responsibilities existing within the CMS.

		Internal vs. External compliance responsibilities	A6-121	The responsibilities split between internal and external compliance topics, existing within the CMS (or equivalent).
B	**Technology in compliance management**	Technology used by the compliance function	B1	The list of technology applications/tools/other that are used by the compliance function.
		AI tools / applications used in compliance management	B1-1	The list of automation/AI applications/tools/other that are used by the compliance function.
		Compliance by Design	B2	How is Compliance by Design addressed within the organization (e.g. to what level and how it is ensured that compliance is embedded in the applications deployed across the organization, from an early stage).
		Predictive models	B3	Predictive models currently in use by the organization towards managing compliance tasks.
		Prescriptive models	B4	Prescriptive models currently in use by the organization towards managing compliance tasks.
		Tools specific to the three lines of defense	B5	The list of technology applications/tools/other that are used at each of the three lines of defense levels to perform their daily work tasks/routines.
C	**People**	Dedicated compliance person/staff per department	C1	Existence of dedicated person per department/line of business/team, in charge with performing compliance duties.
		Compliance reporting structure	C2	Reporting structure and responsibilities of people in charge with compliance duties.
		Tools used by dedicated compliance staff	C3	Applications/digital tools that people in charge with compliance duties use to perform their tasks related to compliance management.
		Training regarding compliance topics	C4	Way and type of training provided to the organization's employees with respect to compliance management or simply compliance topics.
D	**Other**	Silo compliance	D1	The way in which the organization is ensuring that silo compliance (compliance within e.g. departments, functions) is avoided, and therefore compliance-related topics are aligned to the company policies, risk appetite, etc.

		Alignment between functions	D1-1	The way in which different departments/units interact with each other to align on company policies and other compliance-related topics.
		Monitoring-based compliance systems	D2	Understanding the degree to which the organization's compliance system is monitoring-based (using professional auditors/third line of defense), a fact that represents very high costs for the organization.
		Auditing	D2-1	Type and way of auditing and the degree to which audit activities support the compliance management activities of the organization.
		Resources consumed by the organization	D3	Type of resources consumed by the organization to run a CMS in order to break-even on the equation: Resources = Requirements
		Cost of running a compliance system	D3-1	Knowledge on the costs incurred by the organization to run a CMS (covering all the three lines of defense).
E	**New themes and codes**	Relationship with regulator	E1	The influence and involvement of regulators within the activities and decisions related to the management of compliance has a direct correlation to the overall CMS of an organization.
		Global standards or standards coming from national authorities	E2	The influence of global standards or national standards on the compliance management system and the policies an organization adopts and implements within its CMS.
		Collaboration with external parties	E3	The type and form of collaboration with external parties and how it influences, impacts or affects compliance management activities (whether it is vendors, collaborators, partners etc.).
		Data management	E4	Topics related to the management, governance, and other considerations related to data within the organization.
		Cyber security	E5	Topics related to information security and how these affect the compliance policies and procedures of the organization.
		Ethics	E6	The consideration of ethical concerns when elaborating, adopting, operating automation/AI applications/tools.
		Hardware and software (IT) infrastructure	E7	The IT infrastructure (hardware and software) that the organization has, or is about to implement, as this affects the capabilities of the automation/AI applications or tools.

Appendix B – case study 1 data excerpts

Code of Ethics and Business Conduct – excerpt of contents

Definition & Applicability

Vision, Mission & Brand Values

Compliance & Reporting

Violations

Our Standards

- Policies & Procedures
- Nondiscrimination, Diversity & Inclusion
- Harassment-Free Workplace
- Health, Safety & Security
- Fraud Prevention
- Conflicts of Interest
- Acceptance of Gifts
- Protection of Assets
- Financial Statements
- Political & Charitable Activities
- Employment Outside of *the organization*
- Regulatory Compliance
- Antitrust / Competition
- Anti-corruption / Bribery
- Economic Sanctions
- Industry Activities vs. Products & Services

Resources for Assistance (see Table 1.Appendix B)

Table 1.Appendix B

Code of Ethics & Business Conduct	Chief Auditor, General Counsel or VP, PPD
Reporting violations	Legal Services; Internal Audit; PPD Departments; Ethics Hotline (www.iata.ethicspoint.com)
Conditions of employment, diversity, harassment, discrimination, personal information	PPD Department; Deputy General Counsel
Health, Safety, Security	PPD Department; CAP Department; ITS Department
Conflicts of Interest, Acceptance of Gifts, Corruption/ Bribery	Chief Auditor, General Counsel or VP, PPD
Antitrust Compliance	Assistant General Counsel
Anti-Money Laundering Compliance	AD, Regulatory Compliance
Economic Sanctions Compliance	Assistant General Counsel
Legal Policy, Confidential Information	General Counsel
Audit Policy, Fraud Prevention	Chief Auditor
Risk Management Policy	AD, Corporate Risk Management
Corporate Finance Policy, Financial Books & Records	Director, Finance
Administration, Procurement Policy	Director, CAP
Planning, Project Policy	Director, CPS
Information Technology Policy	CIO & Director ITS
People, Performance & Development Policy	VP, PPD
Communication Policy	VP, Corporate Communications

Appendix C – case study 2 data excerpts

Code of Business Conduct – excerpt of contents

1. Ethical values of *the organization*

2. Scope of application

3. Ethical conflict situations

4. Compliance with the law

5. Corporate social responsibility

6. Conflicts of interest

7. Insider trading

8. Competition

9. Confidential information and data protection

   9.1 Confidential information

   9.2 Data protection

10. Accounting and protection of company property

11. Integrity Compliance

    11.1 Bribery, corruption and facilitation payments

    11.2 Gifts, hospitality and invitations

    11.3 Donations, sponsorships and memberships

    11.4 Combating money laundering

12. Foreign trade regulations

    12.1 Embargoes and sanctions

    12.2 Export Controls

13. Discrimination and harassment

14. Communications

14.1 External communications

14.2 Internal communications

14.3 Information and communication tools

Group Compliance Management System – areas covered

- Competition compliance
- Integrity Compliance
- Third Party Due Diligence (TPDD)
- Embargo Compliance / Export Controls
- Capital Market Compliance
- Other topics – e.g.:
    - Code of Conduct
    - Compliance Risk Assessment

Appendix D – invitation to participate in the interview

Dear Ms/Mr X,

I have received your contact details from X (role). I know X from…. I am based in Zurich, and have an aviation and finance / internal audit, as well as most recent data & analytics background.

The main reason I am contacting you, is to enquire if your organization would be interested to be one of the case studies in my research. I am interested in understanding/exploring the topic of Compliance Management Systems as a strategic development in your company. I am very interested to understand your, and your colleagues' perceptions and challenges in deploying and managing a system of compliance, which could or is already enabled by Augmented Intelligence (Artificial Intelligence) applications.

I prepared an introductory background to the research, which I hope gives you a first glimpse at the topic.
Should you find the chance to read through, and believe this is indeed of interest to you and your organization, I'd be happy to provide you with additional information, schedule a first call, or answer any question related to the research, which you might have.

Thank you in advance for your time, I look forward to your feedback.

Here is some background information:

I would like to interview two or three people holding one of the following roles (any variation to these titles is accepted):

- Chief Compliance Officer / Compliance Officer
- Chief Digital Officer / Head of Digital / Digital Manager
- Chief Financial Officer / Head of Finance Operations / Finance Operations Manager
- Head of Digital Innovation
- General Counsel / Head of Legal Affairs
- Chief Technology Officer / Head of IT

The interview should take 1 hour (maximum 1.5 hours if the interview partner has the time capacity), and I would like to conduct it in person.
In addition, I would request some documentation on strategic initiatives in the deployment of AI/automation applications across the organization.

Data collected will be anonymized. Results as well. No names (neither people nor company) will be written in the thesis or subsequent publication. A consent form is to be signed ahead of any data collection (further details below).

Introduction

I am a research student at Edinburgh Napier University, in the Doctorate of Business Administration (DBA) programme. Entering my 3rd year of studies, I am about to start the data collection phase of my research. The doctorate studies in the DBA context, are aimed at finding new knowledge that can also be applied in practice.

I am interested in understanding/exploring the topic of Compliance Management Systems as a strategic development in your company. I am very interested to understand your, and your colleagues' perceptions and challenges in deploying and managing a system of compliance, which could or is already enabled by Augmented Intelligence (Artificial Intelligence) applications. Important to stress is that the research is not about assessing the level of compliance.

Title of the research

Guidelines for Artificial Intelligence-driven Enterprise Compliance Management Systems

Research aim

The aim of the research is to investigate how compliance management systems are strategically set-up in large organisations and to what degree they are supported by Artificial Intelligence (AI) applications, in order to provide conceptual guidelines to such organisations on deploying an enterprise-wide compliance management system enabled by AI, therefore contributing to knowledge as well as practice.

Research objectives

1. To identify the objectives of a compliance management system within organizations by critically reviewing the literature.
2. To analyse the set-up of compliance management systems, as well as the enablers and barriers of AI adoption within large organisations by conducting multiple case study research.
3. To compare findings from practice and theoretical underpinnings, and explore how AI can strategically demonstrate being an enabler of compliance management activities.
4. To provide conceptual guidelines for the set-up of an enterprise-wide compliance management system driven by AI, within large organizations.

Research approach

This research is done using case study as a method. Research is conducted using an abductive approach as the circumstances of the compliance functions within organisations are used to generate tested conclusions about their best possible set-up. Using the abductive approach, collected data is used to identify themes and patterns (open coding process) and create a conceptual framework/guidelines for the best possible fit of compliance systems within organisations.

Data is collected and structured based on the qualitative research methods described. Sources of data are:

- Interviews: semi-structured, open-end encouraged.
- Documents and archival records: these data sources provide a basis for confirming the ‘real’ world of what is to be studied.

The method of analysis pertinent to the data collection used in conjunction with the multiple cases studies design, starts with coding, then is followed by thematic clustering of codes. The coding is based on a step by step approach.

Ethical considerations

The research study is subject to ethical scrutiny, by the ethics committee of Edinburgh Napier University, and as such, an ethics approval has been received by the student.

A participant Information and consent form shall be distributed to participants in the interviews, prior to conducting any data collection for the purpose of the research.

Best regards,
Ana-Maria

Ana-Maria Wall

Appendix E – interview questionnaire

A. General introductory questions:

1. I would like to talk about your organization's strategy in terms of adoption of AI solutions in general, and in particular when it comes to compliance management. The questions of this interview are aimed at revealing the general strategy of the organization for adopting AI-driven technologies to support the CMS.
2. How would you describe and rate the maturity of AI applications/tools existing or about to be adopted in your organization?
3. What do you consider to be the enablers of AI-driven technology adoption?
4. What do you consider to be the barriers of AI-driven technology adoption?
5. How is your organization structured? Please provide an organizational chart if possible.
6. How do you define compliance in your organization?
7. How is the compliance function organized in your firm? Please refer to the Organization Chart.
8. Is each department responsible for its maintaining and responding to compliance requirements?
9. Is there a formal Compliance Management System in your organization?
10. Is there an alignment between how and who addresses internal and external compliance?

B. Technology in compliance management:

1. What technology is currently used by your compliance function?
2. Based on the AI definition provided, what AI technology is currently used by your compliance function?
3. Is Compliance by Design a topic actively addressed? E.g. is it ensured that compliance is embedded in the applications deployed across the organization, from an early stage?
4. Does your organization use any predictive or even prescriptive models, towards managing compliance tasks?
5. Let's talk about the three lines of defense in your organization, and what applications / digital tools they have available to perform their daily work tasks/routines:
    a. Business lines
    b. Support functions
    c. Internal audit

6. Following the financial crisis of 2008, a new field has emerged, called Regtech. Does your organization employ a company to provide Regtech services in any area of the business?

C. People:

1. Is there a dedicated person per department / line of business / team, in charge with performing compliance duties?
    a. If yes, does this person work together with IT (e.g. IT to Business alignment function exists) to bridge the gap between business and technical requirements?
2. To whom do people in charge with compliance duties report?
3. What applications / digital tools do these people use to perform their tasks related to compliance management?
    a. To your knowledge, are these tasks partly or fully automated? Therefore, the role of the persons responsible for compliance activities becoming more of a reviewer/checker/Quality Assurance/monitoring? - "Human in the loop" concept.

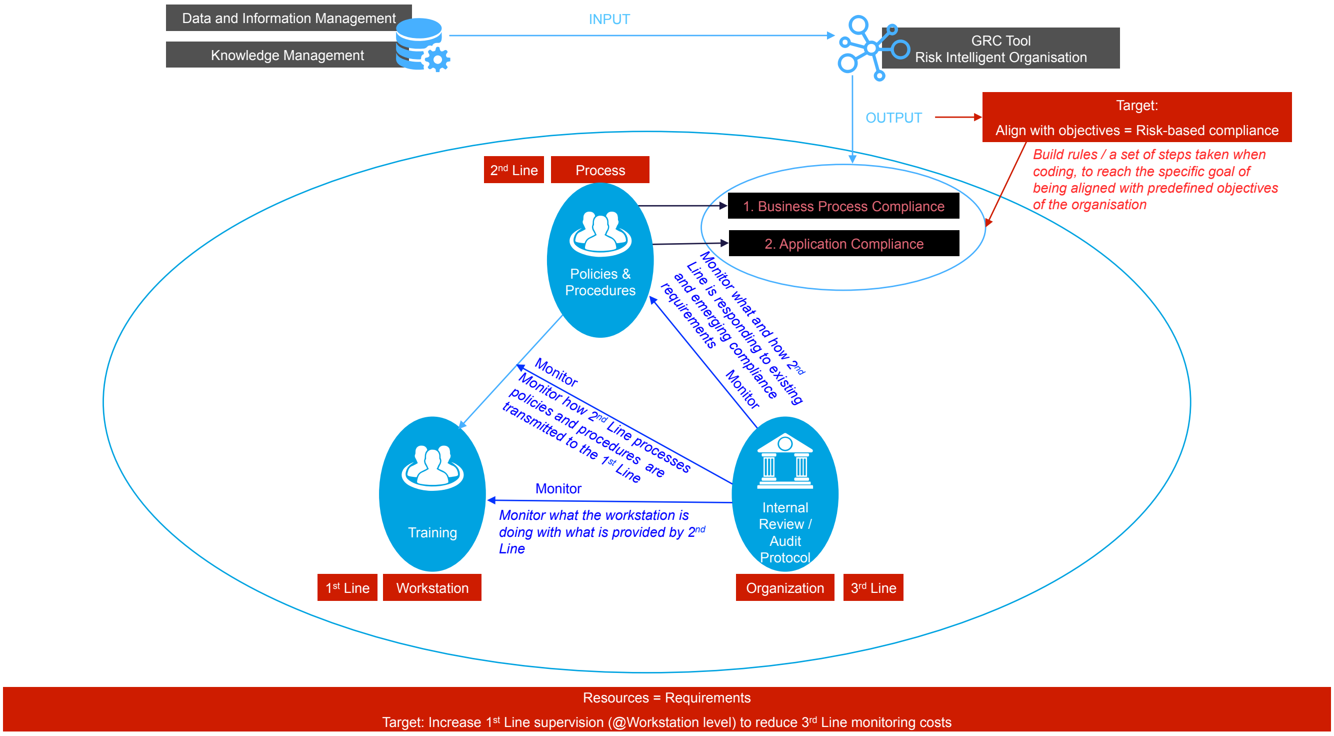
D. Other:

1. Silo compliance as scattered efforts:
    a. Do you implement software / platforms following tight regulatory deadlines?
        i. This tends to lead to silo compliance due to ""go-live"" pressure - how do you deal with this kind of pressure and still integrate the new platforms in the overall landscape and compliance needs?"
2. Most compliance systems are monitoring-based (using professional auditors / third line of defense). This represents very high costs for the organization.
    a. What can you say about this within your organization?
3. What type of resources are consumed by the organization to run a CMS in order to break-even on the equation: resources = requirements
    a. Is this something known to the organizations, and moreover, is it reported on?
    b. Do you know if you invest more resources than needed by your compliance requirements?

Appendix F – matrix of case study documentation

Type of documents					
		Case 1	**Case 2**	**Case 3**	**Comments**
1	Code of conduct	x	x		
2	Meeting minutes		x		
3	Organizational chart		x	x	For Case 2, only the chart of group companies
4	Annual report	x	x	x	For Case 2, only the report of the mother group
5	Job portal		x		
6	Company registrar		x		
7	Investor report			x	
8	Online news	x	x		

Appendix G – CMS ecosystem resulting from literature review


Data and Information Management
Knowledge Management
INPUT
GRC Tool
Risk Intelligent Organisation
OUTPUT
Target:
Align with objectives = Risk-based compliance
Build rules / a set of steps taken when coding, to reach the specific goal of being aligned with predefined objectives of the organisation
2nd Line
Process
Policies & Procedures
1. Business Process Compliance
2. Application Compliance
Monitor what and how 2nd Line is responding to existing and emerging compliance requirements
Monitor
Monitor
Monitor how 2nd Line processes policies and procedures are transmitted to the 1st Line
Training
Monitor
Monitor what the workstation is doing with what is provided by 2nd Line
Internal Review / Audit Protocol
1st Line
Workstation
Organization
3rd Line
Resources = Requirements
Target: Increase 1st Line supervision (@Workstation level) to reduce 3rd Line monitoring costs

Appendix H – writers and their focus in literature

The identified key writers, their articles and papers, year of publication as well as their focus on subjects related to CMS and AI is presented as an overview list in the table below.

Key literature on Compliance Management Systems and Artificial Intelligence

Author	Year	Description	Focus
Langevoort, D. C.	2002	The focus of this paper is to determine what social and cognitive psychology research (the stuff of contemporary behavioural law and economic) has to say about the task of compliance and the contest between hard and soft monitoring strategies.	The behavioural economics of corporate compliance with law
Parker, C.	2003	This paper critically examines the ability of compliance program audits to provide adequate assurance of compliance system performance. The empirical evidence comes from the use of compliance program audits in monitoring compliance with enforceable undertakings agreed upon between companies (that have allegedly breached the law) and the Australian Competition and Consumer Commission and the Australian Securities and Investments Commission.	Corporate Compliance Program Audits
Haynes, A.	2005	The aim of this paper is to analyse how a bank can best succeed while approaching compliance as a risk-based issue. This is done while bearing in mind the various internal departments and external agencies that can impact on, or be impacted by the procedures adopted.	Risk-based compliance

Boland, R.	2006	This article describes the early stages of CMS, and what to look for when choosing a CMS. It lists three basic components of a CMS: 1) A library of applicable requirements. 2) A library of tasks developed from the requirements. 3) A means to administer status reporting and recordkeeping.	Reduce Business Risk with a CMS

Ramanathan, J;
Cohen, R J;
Plassmann, E;
Ramamoorthy, K.
	2007	Written in the IBM Systems Journals, this article claims that runtime audit data that records information such as operational logs represents a key element needed for compliance management. An audit service that manages the life cycle of audit data is thus a critical component of any compliance management system.	This paper focuses exclusively on the use of audit logs for compliance management.

Kumar, V., Pollanen, R., Maheshwari, B.	2008	Challenges faced by companies in enhancing their enterprise resource planning (ERP) systems for compliance with regulatory internal control requirements (specifically those imposed by SOX).	Silo compliance in IT systems as it addresses ERP compliance.
Butler, T., Mcgovern, D.	2009	This paper focuses on the very-much underexplored issue of environmental compliance and risk. The first objective of this exploratory study is to delineate the problems facing GRC and Environmental Health and Safety (EH&S) functions in dealing with environmental regulations globally and to identify how these problems are being solved using Environmental Compliance Management Systems (ECMS). The second objective is to propose a process based conceptual model and related IS framework on the design and adoption of ECMS that will inform future research and, it is hoped, the IS adoption decisions of GRC and EH&S practitioners.	Environmental Compliance Management Systems (ECMS)

Parker, C., & Nielsen, V. L.	2009	This article critically appraises the potential of corporate compliance systems to influence corporate behaviour. The authors differentiate between the adoptions of formal compliance management systems and the way compliance is managed in practice in business organizations by reference to scholarly literature and analysis of survey responses from 999 large Australian businesses about their implementation of competition and consumer protection law compliance systems.	Corporate Compliance Systems structure
Russell, S., Norvig, P. & Davis. E.	2010	Introduction to the theory and practice of artificial intelligence.	Artificial Intelligence
Bamberger, K. A.	2010	This article investigates the accountability challenges posed by technologies of control and suggests specific reform measures for policy makers revisiting the governance of risk.	Risk and regulation in a digital age (technologies of compliance)
Pluta, P.L., Poska, R.	2010	This paper proposes an organized approach to compliance – compliance by design (CbD) documented in a compliance master plan (CMP).	Compliance by design (CbD)
Giampaolo, G. & Musile Tanzi, P.	2011	The purpose of this paper is to find out how effectively implemented are approaches to measure compliance and whether there is a correlation between the measures implementation, financial specialization and international activity. The authors evaluate if the regulatory framework implies a measure cost asymmetry, depending both on the proportionality principle and on the existence of different supervisors with a heterogeneous set of enforcement rules.	Compliance costs in financial services organizations
Elgammal, A., Turetken, O., Heuvel, W.J., Papazoglou, M.	2014	This paper proposes a business process compliance management framework based on Compliance Request Language (CRL), which is formally grounded on temporal logic and enables the abstract pattern-based specification of compliance requirements.	Abstract pattern-based specification of compliance requirements

Gozman, D. & Currie, W.	2014	The purpose of this paper is to understand how institutional changes to the European Union regulatory landscape may affect corresponding institutionalized operational practices within financial organizations.	Rules-based compliance systems in financial organizations
Papazafeiropoulou, A., Spanaki, K.	2015	The aim of this exploratory study is to understand the aspects and the nature of the GRC system following an enterprise systems approach.	The nature of the GRC system
Perezts, M. & Picard, S.	2015	The way compliance with regulations is actually enacted or ''performed'' within organizations instead of merely executed, remains largely under-characterized. A particular interest is given to the work of embedded ethics in this process, as an enabler to partly recouple compliance with the regulated activity.	Embedded ethics in compliance management
Abdullah, N.S., Indulska, M., Sadiq, S	2016	This paper reports on the development of an ontology intended to provide a shared conceptualisation of the compliance management domain for various stakeholders. The ontology is based on input from domain experts and practitioners, validated and refined through eight case studies, and subsequently evaluated for its usability in practice.	Compliance management ontology
Knuplesch, D., Reichert, M., Kumar, A.	2016	This paper presents a comprehensive framework for visually monitoring business process compliance.	Business process compliance monitoring
Kim, S.S, Kim, Y.J.'s	2017	The purpose of this paper is to understand from the knowledge management perspective how the mechanism of different voluntary compliance behaviours works and how information technology is used for compliance management in corporate settings where privacy and security issues are getting critical due to the advancement of big data and artificial intelligence.	Compliance knowledge and compliance support systems for information security compliance behaviour
Butterworth, M.	2018	The question of 'fairness' is an important one, to address the imbalance between big data	The role of fairness in the GDPR

		organisations and individual data subjects, with a number of ethical and social impacts that need to be evaluated in the way the GDPR is addressed by organizations.	framework
Jarrahi, M. H.	2018	This article highlights the complementarity of humans and AI and examines how each can bring their own strength in organizational decision-making processes typically characterized by uncertainty, complexity, and equivocality.	Artificial intelligence and the future of work: Human-AI symbiosis in organizational decision making
Wright, S. A., & Schultz, A. E.	2018	The proposed framework identifies the ethical implications of business automation, highlights best practices, offers recommendations, and uncovers areas for future research.	The rising tide of artificial intelligence and business automation: Developing an ethical framework.
Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., … Williams, M. D.	2019	The study brings together the collective insight from a number of leading expert contributors to highlight the significant opportunities, realistic assessment of impact, challenges and potential research agenda posed by the rapid emergence of AI within a number of domains: business and management, government, public sector, and science and technology. This research offers significant and timely insight to AI technology and its impact on the future of industry and society in general, whilst recognizing the societal and industrial influence on pace and direction of AI development.	Multidisciplinary perspectives on AI emerging challenges, opportunities, and agenda for research, practice and policy
Farrow, E.	2019	Artificial Intelligence origins connect to the human drive to expand our mental and physical capacity, seek advantage, survive and flourish. This paper examines the past 5000 years of AI and applies the future research methodology Causal Layered Analysis	Augmenting human capacity and decision-making; AI evolution through causal layered analysis.

		combined with genealogical analysis.	
Barredo Arrieta, A., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., … Herrera, F.	2020	Explainable AI (XAI) field, which is widely acknowledged as a crucial feature for the practical deployment of AI models. The overview presented in this article examines the existing literature and contributions already done in the field of XAI, including a prospect toward what is yet to be reached.	Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI.