6-18-2022

AI GOVERNANCE: ARE CHIEF AI OFFICERS AND AI RISK OFFICERS NEEDED?

Mathias Schäfer
University of Liechtenstein, mathias.schaefer@students.uni.li

Johannes Schneider
University of Liechtenstein, johannes.schneider@uni.li

Katharina Drechsler
University of Liechtenstein, katharina.drechsler@uni.li

Jan vom Brocke
University of Liechtenstein, jan.vom.brocke@uni.li

AI GOVERNANCE: ARE CHIEF AI OFFICERS AND AI RISK OFFICERS NEEDED?

Research in Progress

Mathias, Schäfer, University of Liechtenstein, Vaduz, Liechtenstein, mathias.schäfer@uni.li

Johannes Schneider, University of Liechtenstein, Vaduz, Liechtenstein, johannes.schneider@uni.li

Katharina Drechsler, University of Liechtenstein, Vaduz, Liechtenstein, katharina.drechsler@uni.li

Jan vom Brocke, University of Liechtenstein, Vaduz, Liechtenstein , jan.vom.brocke@uni.li

Abstract

While AI provides many business opportunities across industries, the organizational implications of AI are still largely unclear. We investigate governance roles related to AI use in practice, and undertake first steps to define the role profiles of a Chief AI Officer (CAIO) and an AI Risk Officer (AIRO). We base our inquiry on two sources: a literature review and evaluative interviews with nine AI professionals from small- and medium-sized companies. We find that, whereas the roles and activities associated with the CAIO and AIRO are commonly deemed relevant for such companies in the long run, today only a few companies have implemented them. Especially the creation of the CAIO position seems justified, due to the complexity of AI and the need for extensive interaction and coordination related to AI governance.

Keywords: AI, governance, roles, organization, risk.

1 Introduction

Artificial intelligence (AI) has undoubtedly reshaped our modern world. It is one of the central technological achievements of the past 20 years and AI will continue to shape the way we work and live. Davenport (2018) shows that an overwhelming majority of company leaders believe that their organizations will be substantially transformed in the next years by AI, even if those leaders themselves do not have much knowledge about artificial intelligence. There are claims from developers and companies that highlight and sometimes exaggerate AI's benefits and impact (Duan, Edwards & Dwivedi, 2019). This is worrisome, since along with the rise of AI, many non-technical challenges, such as risk management and ethical dilemmas, have come up.

Without governance mechanisms that enable a proper supervision and risk evaluation structure, the use of AI might be a backlash for companies causing additional costs. Recent scandals have shown that neglecting AI governance can lead to a variety of damages for companies, such as business disruptions, systematically wrong or biased predictions, reputational damage, client withdrawal or sometimes even the payment of large fines for legal violations (Whittaker et al., 2018). Adequate structural governance mechanisms might help in controlling risks and leveraging AI's potential. However, the governance of AI poses novel challenges compared to classical IT governance. When focusing on artifacts to be governed, AI governance can be seen as governing (i) data used for training (AI) models, (ii) models and (iii) systems containing these models (Schneider et al., 2020). Data governance comes with new

challenges compared to IT governance (Abraham et al., 2019; Brown & Grant, 2005). Model governance also adds novel aspects compared to software governance (Sridhar et al., 2018).

These differences can be understood by looking at characteristics of AI. AI can be seen as a moving frontier that involves autonomy (acting without human intervention), learning (from data) and inscrutability (being difficult to understand) (Berente et al., 2021). They distinguish AI from other digital technologies, such as blockchain whose adoption can also lead to competitive advantages (Werner et al., 2021). Other digital technologies are seemingly easier to confine and understand and, thus, in lesser need of extensive governance. This difficulty of understanding AI has given rise to research on explainable AI (Meske et al., 2021), since security and safety risks are hard to assess and control without a thorough understanding.

The complexity and importance of AI for many businesses might call for creating a new managerial role, such as a Chief AI Officer (CAIO). At the same time, AIs' obscurity, arising from its autonomy in operation and learning to make decisions from data, rather than being programmed explicitly, can contribute to increased risk that necessitates an AI Risk Officer (AIRO). Minimising the potential harms and costs associated with radically new technologies may require a very different mindset than maximising profits and deriving business value from AI, which also calls for separate roles for managing risk and ensuring value generation from AI. Though AI poses new challenges, it is unclear to what extent new roles are needed and, if so, what their responsibilities should be.

Existing scientific literature lacks an elusive discussion of the role description of professionals dedicated to AI governance, possibly, since these roles as well as other governance mechanisms, such as AI Centres of Excellence (Davenport, 2021; Minevich, 2021), are still rare even among technology-oriented companies. A study by Teradata (2020) highlights that within only 8% of companies the post of a CAIO exists. Thus, in most organizations AI is governed by the Chief Information Officer (CIO) or the Chief Technology Officer (CTO) and only plays a subordinate role among other technologies. However, with the growing importance of AI for companies and due to its complexity, there are indicators that creation of a dedicated CAIO role is gaining popularity. Alkashri, Siyam & Alqaryouti (2020) state that the "CAIO will help the organization getting the maximum out of AI technologies implementations in all areas (p. 669)", whereas Nachtigall (2020) highlights that 62% of surveyed people expect that AI will be so important in the future that they have to hire a CAIO.

Others point to the importance of expanding or re-assembling employees' professional roles (Chakraborty, 2019). One such re-assembling could take place in the risk department and lead to the rise of the AIRO. Even though the AIRO has not been well studied, Hodge (2020) believes that its importance will grow and that AIROs will take a "strategic and consultative role in their organizations (p. 29)". However, risk management of AI could also be split among other roles. For instance, security risks could be managed by the chief security information officer, who may take over "the responsibility for designing, implementing and managing security safeguards and countermeasures based on risk management" (Maynard et al. 2018).

Against this backdrop, this research-in-progress aims to derive and assess new managerial roles that emerge as structural governance mechanisms to minimize risks of AI and provide general oversight of AI. To this end, we synthesize the potential profile of a CAIO and an AIRO based on extant literature, covering research on such roles as well as a larger body of works on AI management and governance. To evaluate the profiles of these roles and determine on a qualitative level if such roles are needed, we conducted nine interviews with AI experts. As we lay out in our research method, the presented profiles based on a first round of interviews need more refinement and contrasting to existing roles but provide a first conceptualization of CAIO's and AIRO's profiles. These roles are important since the overall AI governance is challenging due to the complexity and benefits of AI that have yet to be leveraged on a broad level (Ransbotham et al., 2020). Due to the transformational nature of AI, potential risks for organizations are extensive and should be well-managed.

2 Background

Research on IT governance, defined as the "framework for decision rights and accountabilities to encourage desirable behavior in the use of IT" (Weill 2004, p.3), has a long tradition in the Information Systems field (Brown, 2005). Earlier research predominantly focused on the forms of IT governance (e.g., Brown 1997; Brown & Magill, 1994) and contingencies of IT governance (e.g., Sambamurthy & Zmud, 1999). Over time, this focus shifted to exploring the influence of specific structural, procedural, and relational governance mechanisms (e.g., Bradley et al., 2012; Huang et al., 2010).

One important component of IT governance is the role of executives. Information Systems research has especially studied the role of the chief information officer (CIO) (Balocco, Ciappini & Rangone, 2013; Drechsler, 2020). While CIOs were traditionally focused on establishing cost-effective IT infrastructure (Grover et al., 1993), CIOs' responsibilities were gradually extended to include IT strategy and a focus on creating and envisioning business value through IT (Chun & Mooney, 2009). CIOs have been shown to drive organizational performance, for instance, by impacting IT strategic alignment (Karahanna & Preston, 2013) and establishing the perception of an organization's superior IT capability (Lim et al., 2013).

However, the rise of digital technologies, such as the internet of things, platforms, and artificial intelligence, are disrupting the established perspective on IT governance and the leadership role of CIOs (Fitzgerald et al., 2014; Weill & Woerner, 2013). To successfully face these challenges, numerous companies have reconsidered their governance structures and appointed new managerial roles, such as the Chief Digital Officer (CDO) (Tumbas et al., 2017, Drechsler, Wagner & Reibenspiess 2019). CDOs are positioned at the intersection between business and IT to coordinate and orchestrate digital initiatives, such as the development of digital innovation, across the company. An alternative executive position constitutes the Chief Technology Officer (CTO), who is responsible for the integration of technology into companies' strategy (Smith 2003). Yet, depending on the industry a company is positioned in, the CTO's focus may be quite removed from questions regarding AI.

The complex questions surrounding the use of AI, which encompass technical, ethical, risk and business issues, require a combination of skills that CIOs, CDOs and CTOs do not typically possess. As a result, the question arises as to whether new managerial roles are needed for organizations to use AI to their advantage. In the following, we present findings of extant literature on the AI Risk Officer and Chief AI Officer.

2.1 AI Risk Officer

A common understanding in AI-related legislature is that every company is fully liable for damages caused by its own AI systems. Hence potential damages need to be monitored closely (Lee, 2020). Important aims are ensuring continuity, market safety, customer protection and market integrity (Lee, 2020). Drafting and supervising the risk strategy is one of the main tasks of the risk department and, possibly, the new role of the AIRO. Managing AI risk requires dealing with external risks, and being held accountable by third parties, e.g., regulators, auditors, media, and consumers. This can be seen as a multi-step plan that consists of various analyses that indicate how much risk a company can take in which area. The types of risk are diverse, including legal (possibly differing by country), environmental, financial and reputational risks (Cheatham et al., 2019). Societal risks, e.g., related to replacing workers by AI, are typically not directly included, since they do not impact profits but they might manifest as reputational risk.

The risk strategy provides a holistic overview of interdependencies between different risk categories, so that the aforementioned thresholds and benchmarks can be well-reasoned (Utne, Hokstad & Vatn, 2011). The AIRO needs to exchange information with top-level management and other departments to check if the demanded risk thresholds are plausible, feasible and in line with business strategy.

Commonly known AI specific risks are related to data, e.g., due to noisy or biased data, and models, e.g., security issues due to vulnerability to attacks, opacity of models and misinterpretations by humans in the loop. Even if an AI system was properly developed, trained with non-biased data and tested, it

might still pose a threat or at least a liability to the company. This happens when the relationship between the included risk factors and the outcome changes after model development (Lynas, 2010). The strategic orientation and the risk appetite of a company might also change over time (Malali, 2020).

Black et al. (2018) distinguish three different categories for model risks: (i) fundamental errors, (ii) outputs deviating from the design objectives and intended business uses, and (iii) incorrect or inappropriate use. The first type of model risk refers to misspecification of the model itself. It should be discovered during audits or testing, which are not necessarily tasks of risk management. Whether an output deviates from the intended business use cannot be decided without being aware of the business activities. It constitutes an 'operational' risk, that is, a residual risk not intrinsically arising from a system. Put differently, an operational risk only becomes visible during practical usage ('operations') (Power, 2005). Consequently, operational risks cannot be detected by an audit in an isolated environment. Detection relies on monitoring a deployed model. To be able to observe the risk of inaccurate outputs, the model's outputs must be viewed against the business and the risk strategy to assess whether the risks are compliant with the strategy and whether there are economical risks, for instance, whether the costs saved by AI-based automation compensate for potential costs due to failures.

The model risk of "incorrect or inappropriate use" also requires in-depth analyses. It refers to human errors in using the model, which should not be underestimated, as human wrong-doing can cause high damage to the company (Bevilacqua, 2018). To understand the potential of human errors, the risk department must closely monitor how the AI system is used (Islam et al., 2018). Unexpected routines might emerge that have not been covered by audits or testing, with a few routines containing inherent dangers for the involved people. Mannes (2020) points out that regular safety audits are necessary, especially if physical damage is possible. If strong safety concerns persist, the risk department might even recommend forgoing machine learning algorithms for specific projects (Burrell, 2016). Furthermore, there is also the imminent risk of external intrusion, e.g., by malicious hackers that might gain unauthorized access to models and data as well as to attacks on the AI system itself.

AIROs should come up with a model risk policy. It defines the roles and responsibilities of stakeholders in the model risk management process and modeling standards that set out requirements for the development, validation, and use of models (Black et al., 2018). The model risk policy should not only be generic, but it should also define acceptable and non-acceptable risks for each model separately. It is important to justify risk thresholds, as otherwise, misunderstandings might arise. The model risk policy needs to be provided to both the data and the technology representatives. Furthermore, the policy also includes aspects of what should be tested during an audit, i.e., an audit committee needs to be informed about the model risk policy as well. Control design principles (Ernest & Young, 2018) could be used as a basis for describing the different aspects of the model risk policy, such as assessing algorithms' fitness for specific uses, testing, preventive controls (e.g., kill-switches to turn off AI), resiliency testing (e.g., against adversarial attacks), human control/override mechanisms, compliance with rules and regulations, organizational code of conduct, and ecosystem monitoring with emphasis on risks. Also, training measures combined with actions to raise awareness of data security issues can be included in such a risk policy (Trunk, Birkel & Hartmann, 2020).

The model risk policy should also be submitted to the top-level management if organizational measures are included. Employees and external stakeholders might be equally interested in the current risks within the AI system. For this reason, Kurshan, Shen & Chen (2020) suggest conducting and publishing model risk ratings. These ratings complement the risk audit results by providing a concise overview of which tests have been done to the AI system and what the results are. It should consider the risk of individual models as well as potential adversarial effects if they are linked together, i.e., the so-called interconnected risk (Asermely, 2018).

The AIRO should be part of the risk committee in the organizational hierarchy, which oversees the different departments and their specific risks. Forming such an interdisciplinary risk committee is desirable, as it helps to harmonize risk standards across the company, promotes transparency and contributes to overcoming organizational silos (Al-Hadi, Hasan & Habib, 2016).

2.2 Chief AI Officer

Top-level management should care for strategic leadership (including that of AI), develop the corporate strategy, and decide what measures need to be taken to keep the company competitive (Hilb, 2020). The CAIO can support the implementation of management decisions and translate them into precise requirements and project goals that are easily understood (by AI experts).

The CAIO requires both AI and business understanding and often social skills. Magistretti, Dell'Era & Petruzzelli (2019) suggest that every company should increase their AI skills by organizing external research activities, e.g., in the form of a long-lasting contractual partnership with other companies, participation in university programs to get new scientific insights or even organize hackathons to acquire numerous possible solutions to a specified problem. Depending on the company's industry, the CAIO might embed (external) domain-specific experts to support AI activities, either on a contractual or a permanent basis. This is because these experts with large domain knowledge can strongly contribute to conceptualizing AI models or checking the plausibility of a model, even if they do not have an AI background. Cooperation can also focus on companies within the same industry, governance bodies (Ho, Ali & Caals, 2020) or, in the case of financial institutions, FinTechs (Harrison, Duarte & Hall, 2018). Organizing the AI knowledge within a knowledge management system or also in the form of knowledge pills can be valuable (Drewniak, 2020).

Another central management task that the CAIO could potentially take over is the development and realization of creative workplace culture (Patterson, 2017). A CAIO might find it easier than other managerial roles to take the cultural and organizational specifications of the AI workforce into account and merge them with the general corporate culture. Even though there needs to be a clear hierarchy established to ensure responsibility and avoid chaos (Zerfass, Hagelstein & Tench, 2020), there must be a culture that everyone feels invited to come up with flaws or suggestions concerning a model (Black et al., 2018). If there is too much pressure on the employees, they could abstain from coming forward if they have questions or discover a problem or misconception, e.g., regarding AI. The CAIO should act as a facilitator and promote an open exchange. Possible employee involvement methods are, for example, the usage of voting or aggregation methods to allow collective and mutually accepted decision-making (Lee et al., 2019). Relating to culture, the CAIO is also in a good position to promote intrapreneurship. This concept should boost working performance by encouraging the workers to form teams and compete against each other, with the best team receiving a reward (Watson et al., 2021). To realize management-formulated aims, a CAIO could encourage intrapreneurship to foster creating, exploiting, and evaluating innovative ideas (Haefner et al., 2021).

AI Risk Officer	**Chief AI Officer**
Aim: risk identification, reduction and prevention **Activities:** establish risk indicators, failure mode guidelines, human error analysis, auditor supervision, development of company-wide risk strategy, model risk policy and rating	**Aim**: AI-business alignment and company leadership **Activities:** cooperation with externals, cooperation IT/business, AI-related strategy interpretation, AI implementation supervision, intrapreneurship promotion, development of model implementation policy and stakeholder report

Figure 1: Framework covering the role of an AI Risk Officer (left) and a Chief AI Officer (right)

The CAIO should provide a model implementation policy. For a specific project, it should clearly state what the desired model should do (or not do) and where attention should be paid to during implementation. Such a policy serves as a means for control over data and models and their use (Palczewska et al., 2013). It outlines the business needs that an AI solution should cover, and it potentially contains a description of relevant legal and ethical principles that must be considered. For better understanding, a stakeholder map might also be included to highlight the needs and interests of different stakeholder groups (Raji et al., 2020). Other potential content includes a depiction of structural vulnerabilities, a review of what has already been done, and the relevant perspectives (Raji et al., 2020). In addition to that, further information like resource restrictions, potential external support or time

horizons can be included. Figure 1 presents the derived framework for AI Risk Officer and Chief AI Officer role covering aims and activities.

3 Research Method

We first derive role descriptions based on a synthesis of existing literature focusing on roles such as 'chief artificial intelligence officer', 'ai risk officer' or 'ai ethics officer'. Since literature was sparse we searched more broadly in a qualitative, narrative manner (King, 2005) for literature related to 'artificial intelligence governance', 'model governance'. The identified research articles were then carefully screened for descriptions and findings regarding AI governance roles. All relevant information was extracted and then coded based on an open coding process (Wolfswinkel et al. 2013). Applying this coding approach iteratively, we derived preliminary concepts describing the different roles relevant for AI governance. We also included a few non-peer-reviewed articles from sources such as MIT Sloan, Ernest & Young and SAS. Note that the findings of these articles were only included in this paper, after we verified the derived role profiles through expert interviews.

We then validated and refined these role descriptions through semi-structured interviews. We decided on semi-structured interviews in order to conduct a thorough analysis, where we compared the main statements and discussed topics across the interviews. Each interview followed a pre-specified guideline, but was also adapted flexibly when necessary to allow interviewees to voice alternative opinions and new thoughts. This enabled the inclusion of new aspects within the role descriptions, which had not been covered by existing literature or were wrongly considered unimportant before (Van den Berg & Struwig, 2017). As a next step, the refined role descriptions were contrasted in more detail against established roles that may be responsible for AI governance in some companies, such as CIO and CDO. AI governance roles were also compared to each other. The refined role descriptions were improved and validated using additional interviews.

So far, we have conducted the first round of interviews and refined the role descriptions based on nine interviews with an average length of about 30 minutes with interviewees from Austria, Switzerland and Germany. Interview partners were selected based on their expertise in artificial intelligence. Four interviewees were researchers at universities or public research institutions with a focus on AI. Two interviewees ran companies that consulted other companies on the benefits and challenges of implementing AI systems internally. The remaining interviewees were employed by private or public organizations and ranged from the CEO of a medium-sized AI solutions company to an AI consultant. The expertise of the interviewees varied from a focus on AI in marketing to ethical aspects of AI. The interviews covered the interviewees' professional role, especially concerning AI. Subsequently, the interviewees assessed the governance of AI in general and the professional roles related to AI governance in particular. More specifically, interviewees were asked to evaluate and share their opinions on the proposed role profiles derived from literature. We also asked interviewees whether they saw a need for companies using AI as part of their business activities to have designated AIROs and/or CAIOs. We also asked interviewees to assess the responsibilities and tasks of the two roles.

After completing the expert interviews, the collected statements were transcribed, analyzed, and embedded into the context of the research topic (Azevedo et al., 2017). To do so, Myers (2004) suggests applying the so-called hermeneutic approach, which allows the comparison of various opinions across different interviews to reach a comprehensive understanding of the statements presented by the various experts. For further insights, this approach was supported by semiotics-based analysis, which categorizes statements into various topics (De la Croix, Barrett & Stenfors, 2018). Consequently, semiotics allows detecting the frequency of a certain concept recurring within the interviews, which indicates being considered important by the interviewee or not. Thus, topics that appear regularly might be elevated to a more prominent place. The results of these interviews were integrated into the job role descriptions.

4 Preliminary Findings

Our findings indicate that interviewees perceived the characterization of the professional roles presented to them (see Figure 1) well. With respect to the roles' aims, activities, deliverables, none of them was deemed irrelevant or ill-placed. Additionally, interviewees extended and detailed some of the existing points, e.g., mentioning how data can be offered for model training within the organization (which is covered by "cooperation with business" in Figure 1). Overall, interviewees also put large emphasis on the financial strain the roles entail, the interdisciplinary nature of the roles, and exaggerated hype surrounding AI in organizations. Interviewees provided additional aspects - not part of the (original) framework – regarding the role of the AIRO. For risks, two interviewees mentioned the risk associated with not meeting business goals, i.e., having a poor cost-benefit ratio. At the same time, one interviewee also mentioned risks related to intellectual property protection and violation, e.g., due to patent rights. The AIRO and risk management were commonly associated with other AI governance dimensions such as law (by three interviewees), ethics and testing (each by two interviewees). For the CAIO no explicit connections to other roles were stated, but multiple interviewees stated its overarching role.

Concerning the need for dedicated roles for an AIRO and a CAIO, it can be summarized that the demand was perceived to be limited, particularly for small- and medium-sized companies, but was expected to grow. Four interviewees said it was too early for the CAIO or that such a role would evolve slowly over time. While one interviewee saw no need, four interviewees were in favor, as outlined in the following interview excerpt:

"The bundling of responsibility in a large company for these types of issues, which can include AI, but also more comprehensively Big Data in general, is certainly necessary, because for meaningful applications in the company you have to act on different levels. First, this is infrastructure and the question of how I want to handle data in the first place, how I want to make it available for my modeling. The second is the topic of process integration, and the third for me is very much the topic of business use and business development. […] When all three dimensions are considered, a company needs to have its areas of responsibility, which are brought together in a single person." (Interviewee 8).

As a reason in favor, interviewees mentioned that a CAIO helps to communicate the relevance of AI to employees and stakeholders and that bundling the responsibility is needed. This is exemplified in the following excerpt:

"The symbolic effect is very important when you do a project. [...] The importance is underlined when I have AI represented centrally in the company." (Interviewee 1)

As prerequisites for a CAIO, interviewees mentioned that AI should play a substantial role in a company, e.g., many AI projects should be conducted. Furthermore, commitment, a dedicated budget and a strategy concerning AI should be in place. General concerns were financial strain due to the additional role, difficulty of recruiting a suitable CAIO and the fact that a CAIO is often not backed by a division (due to his or her interdisciplinary role) requiring a clear answer to the question of what a CAIO is and does. These concerns are illustrated in the following interview excerpt:

C-level people are certain types [of people]. They make decisions. They rule a company. What would a chief AI officer be? That would be a king almost without a country. He hardly has a division behind him. He has almost no budget. He would be a supplicant to almost all his colleagues. He would formally be at the top, but he would have no possibility to implement anything." (Interviewee 3)

Furthermore, it was stated that AI might be overhyped and, thus, a dedicated role might not be needed (yet). For the CAIO, it was voiced by three interviewees that his or her responsibilities could be handled by a CTO (in combination with a CIO). For the AIRO, replies were less supportive, though four interviewees also confirmed the value of an AIRO. For once, the value of risk management was questioned by one interviewee, indicating that risk estimates (including their likelihood and impact) are often only educated guesses. Furthermore, as for the CAIO, concerns with respect to costs of a risk manager were uttered, suggesting that multiple existing roles could perform risk management:

"*Let's say we can't afford the AI Risk Officer and we can't afford the AI Risk Committee because I'm a small company, but my data scientist could still do that task as well as manage risks because he also has a basic understanding of risk.*" (Interviewee 9)

5 Limitations and Discussion

This research-in-progress presents a first characterization of new managerial roles as structural governance mechanisms to minimize risks of AI and provide general oversight of AI. We find that the CAIO leads company efforts to align AI projects with the organization's overall business goals, while also managing ethical concerns. The AIRO is focused on identifying, reducing and preventing risk factors associated with the implementation of AI. In interviews with AI experts, we found that current sentiment towards these roles is mixed. While some interviewees see the need for such roles, especially in larger organizations, others voiced that the role of the CAIO and AIRO may be promising for the future.

At the same time, we are also aware of some of the limitations of our research. Our interviewees were mainly from German-speaking countries and small- to medium-sized organizations. It remains to be clarified to what extent these role profiles differ according to factors such as company size, technology maturity and type of AI usage. While our interviewees were all AI experts with significant work experience and often being familiar with governance aspects of multiple companies, they themselves were not upholding governance roles. In future work, we aim to include interviewees with governance focus (and, ideally, also AI expertise). Moreover, we would like to extend the study to a multi-case study, covering not only AI roles individually but also their embedding in larger governance structures of AI. The ongoing evolution of AI, including technical, legal and societal aspects, highlights that our view on role profiles is transcendent in terms of their responsibilities, aims and deliverables and the need for such roles, which is likely to grow in the future.

The CAIO is part of the top management. As our responses indicate, his or her role is closely linked to a CTO or CIO, and their exact separation is part of future research. An important aspect of a CAIO (arguably more than for a CTO/CIO) is the interaction with external partners. Such interaction might be needed more for AI than other technologies for multiple reasons. For instance, many companies that stem from industries lacking AI expertise are likely to employ AI in the future. A CAIO might also promote and support the adoption of AI, which might call for new forms of intrapreneurship. However, such initiatives might diminish in importance or even cease to exist once applications of AI become more mature and are better understood.

In summary, our study shows that an AIRO needs an understanding of a large group of stakeholders and the emerging legal, ethical, and technical aspects of AI, since risks are associated with failure to comply with legal standards, ethical misconduct that might be traced back to issues in data, model building and testing. In particular, we feel that aside from economical aspects, great care should be taken to assess risks related to human well-being, e.g., failure mode analysis and human error analysis. In the future, it would be interesting to contrast an AIRO with an AI ethics officer, which might focus more on societal risks.

6 Conclusions

AI is evolving quickly with growing applications in many different industries. As AI is changing from hype to reality by providing value to a business, its risks become more prominent, demanding changes to existing organizational structures. New roles such as Chief AI Officer or AI Risk Officer might be needed in the near future. Our work provides first steps towards such role descriptions.

References

Abraham, R., Schneider, J., Vom Brocke, J. (2019). Data governance: A conceptual framework, structured review, and research agenda. International Journal of Information Management, 49, 424-438.

Al-Hadi, A., Hasan, M. M., Habib, A. (2016). Risk committee, firm life cycle, and market risk disclosures. Corporate Governance: An International Review, 24(2), 145-170.

Alkashri, Z., Siyam, N., Alqaryouti, O. (2020). A detailed survey of Artificial Intelligence and Software Engineering: Emergent Issues. In International Conference on Inventive Systems and Control (ICISC), 666-672.

Asermely, D. (2018). Machine Learning Model Governance [Online report]. SAS. Retrieved from https://www.sas.com/en/whitepapers/machine-learning-model-governance-110666.html

Azevedo, V., Carvalho, M., Fernandes-Costa, F., Mesquita, S., Soares, J., Teixeira, F., Maia, Â. Interview transcription (2017). Conceptual issues, practical guidelines, and challenges. Revista de Enfermagem Referência, 4(14), 159-167.

Balocco, R., Ciappini, A., Rangone, A. (2013) ICT Governance: A Reference Framework. Information Systems Management, 30(2), 150-167

Berente, N., Gu, B., Recker, J., & Santhanam, R. (2021). Managing Artificial Intelligence. MIS Quarterly, 45(3).

Bevilacqua, M., Ciarapica, F. E. (2018). Human factor risk management in the process industry: A case study. Reliability Engineering & System Safety, 169(1), 149-159.

Black, R., Tsanakas, A., Smith, A. D., Beck, M. B., Maclugash, I. D., Grewal, J., ... Lim, Z. (2018). Model risk: illuminating the black box. British Actuarial Journal, 23.

Brown, C. V. (1997). Examining the Emergence of Hybrid Governance Solutions: Evidence from A Single Case Site. Information Systems Research, 8(1), 69-94.

Brown, A. E., & Grant, G. G. (2005). Framing the frameworks: A review of IT governance research. Communications of the Association for Information Systems, 15(1), 38

Brown, C. V., and Magill, S. L. (1994). Alignment of the IS Functions with the Enterprise: Toward a Model of Antecedents. MIS Quarterly, 18(4), 371-404.

Burrell, J. (2016).How the machine 'thinks': Understanding opacity in machine learning algorithms. Big Data & Society, 3(1), 1-12.

Chakraborty, D., McGovern, M. E. (2019). NDE 4.0: Smart NDE. In IEEE international conference on prognostics and health management (ICPHM),1-8.

Cheatham, B., Javanmardian, K., & Samandari, H. (2019). Confronting the risks of artificial intelligence. McKinsey Quarterly, 2, 38.

Chun, M., and Mooney, J. (2009). CIO Roles and Responsibilities: Twenty-Five Years of Evolution and Change. Information & Management 46(6), 323–334.

Davenport, T. H., Foutty, J. (2018). AI-Driven Leadership. MIT Sloan Management Review.

Davenport, T. H. (2021). Enterprise Adoption and Management of Artificial Intelligence. Management and Business Review.

Drechsler, K. (2020). Information Systems Executives : A Review and Research Agenda. Proceedings of the Twenty-Eighth European Conference on Information Systems, 1–16.

Drechsler, K., Wagner, H.-T., & Reibenspiess, V. (2019). Risk and Return of Chief Digital Officers ' Appointment – An Event Study. Proceedings of the 40th International Conference on Information Systems , 1–17.

De la Croix, A., Barrett, A., Stenfors, T. (2018). How to … do research interviews in different ways. The Clinical Teacher, 15(6), 1-6.

Drewniak, Z., Posadzinska, I. (2020). Learning and development tools and the innovative potential of artificial intelligence companies. European Research Studies Journal, 23(2), 388-404.

Duan, Y., Edwards, J. S., Dwivedi, Y. K. (2019). Artificial intelligence for decision making in the era of Big Data–evolution, challenges and research agenda. International Journal of Information Management, 48(1), 63-71.

Ernest & Young. (2018). Building the right governance model for AI/ML [Online document]. Retrieved from https://assets.ey.com/content/dam/ey-sites/ey-com/en_us/topics/financial-services/ey-building-the-right-governance-model.pdf?download

Fitzgerald, M., Kruschwitz, N., Bonnet, D., and Welch, M. (2014). Embracing Digital Technology - A New Strategic Imperative. MIT Sloan Management Review, 55(2), 1–12.

Grover, V., Jeong, S. R., Kettinger, W. J., & Lee, C. C. (1993). The chief information officer: A study of managerial roles. Journal of Management Information Systems, 10(2), 107-130.

Haefner, N., Wincent, J., Parida, V., Gassmann, O. (2021). Artificial intelligence and innovation management: A review, framework, and research agenda. Technological Forecasting and Social Change, 162, 1-10.

Harrison, G., Duarte, N., Hall, J. (2018). Where's the Bias? Developing Effective Model Governance. In Proceedings of the Neural Information Processing Systems.

Hilb, M. (2020). Toward artificial governance? The role of artificial intelligence in shaping the future of corporate governance. Journal of Management and Governance, 24(4), 851-870.

Ho, C. W., Ali, J., Caals, K. (2020). Ensuring trustworthy use of artificial intelligence and big data analytics in health insurance. Bulletin of the World Health Organization, 98(4), 263-270.

Hodge, N. (2020).The Evolution of the Risk Manager. Risk Management, 67(2), 24-29.

Huang, R., Zmud, R. W., and Price, R. L. (2010). Influencing the Effectiveness of IT Governance Practices through Steering Committees and Communication Policies. European Journal of Information Systems, 19(3), 288-302.

Islam, R., Khan, F., Abbassi, R., Garaniya, V. (2018). Human error probability assessment during maintenance activities of marine systems. Safety and Health at Work, 9(1), 42-52.

Karahanna, E., and Preston, D. (2013). The Effect of Social Capital of the Relationship between the Cio and Top Management Team on Firm Performance. Journal of Management Information Systems, 30(1), 15–55.

King, W. R., & He, J. (2005). Understanding the role and methods of meta-analysis in IS research. Communications of the Association for Information Systems, 16(1), 32.

Kurshan, E., Shen, H., Chen, J. (2020). Towards Self-Regulating AI: Challenges and Opportunities of AI Model Governance in Financial Services. In Proceedings of the First ACM International Conference on AI in Finance

Lee, J. (2020). Access to Finance for Artificial Intelligence Regulation in the Financial Services Industry. European Business Organization Law Review, 21(4), 731-757.

Lee, M. K., Kusbit, D., Kahng, A., Kim, J. T., Yuan, X., Chan, A., ... Procaccia, A. D. (2019). We Build AI: Participatory framework for algorithmic governance. Proceedings of the ACM on Human-Computer Interaction, 3(1), 1-35.

Lim, J. H., Stratopoulos, T., and Wirjanto, T. (2013). Sustainability of a Firm's Reputation for Information Technology Capability: The Role of Senior It Executives. Journal of Management Information Systems, 30(1), 57–95.

Lynas, N., Mays, E. (2010). Structuring an efficient program for model governance. The RMA Journal, 92(6), 44-49.

Magistretti, S., Dell'Era, C., Petruzzelli, A. M. (2019). How intelligent is Watson? Enabling digital transformation through artificial intelligence. Business Horizons, 62(6), 819-829.

Malali, A. B., Gopalakrishnan, S. (2020). Application of Artificial Intelligence and Its PoweredTechnologies in the Indian Banking and Financial Industry: An Overview. IOSR Journal of Humanities and Social Science, 25(4), 55-60.

Mannes, A. (2020). Governance, Risk, and Artificial Intelligence. AI Magazine, 41(1), 61-69

Maynard, S., Onibere, M., & Ahmad, A. (2018). Defining the strategic role of the chief information security officer. Pacific Asia Journal of the Association for Information Systems, 10(3), 3.

Meske, C., Bunde, E., Schneider, J., & Gersch, M. (2021). Explainable artificial intelligence: objectives, stakeholders, and future research opportunities. Information Systems Management, 1-11.

Minevich, M. (2021). AI Centers of Excellence Accelerate AI Industry Adoption". Retrieved from https://www.forbes.com/sites/markminevich/2021/06/19/ai-centers-of-excellence-accelerate-ai-industry-adoption/

Myers, M. D. (2004). Hermeneutics in information systems research. Social theory and philosophy for information systems, 103-128.

Nachtigall, K. (2020). Neue Rolle des Chief AI Officers gefordert. AI Trendletter. Retrieved from https://www.sigs-datacom.de/trendletter/15-neue-rolle-des-chief-ai-officers-gefordert.html

Palczewska, A., Fu, X., Trundle, P., Yang, L., Neagu, D., Ridley, M., Travis, K. (2013).Towards model governance in predictive toxicology. International Journal of Information Management, 33(3), 567-582.

Patterson, K. (2017). Governance in the age of automation. New Zealand Business + Management, 17, 22-23 .

Power, M. (2005). "The invention of operational risk." Review of International Political Economy 12, no. 4, 577-599.

Raji, I. D., Smart, A., White, R. N., Mitchell, M., Gebru, T., Hutchinson, B., ... Barnes, P. (2020). Closing the AI accountability gap: defining an end-to-end framework for internal algorithmic auditing. In Proceedings of Conference on Fairness, Accountability, and Transparency (pp. 33-44).

Ransbotham, S., Khodabandeh, S., Kiron, D., Candelon, F., Chu, M., & LaFountain, B. (2020). Are you making the most of your relationship with ai? https://www.bcg.com/publications/2020/is-your-company -embracing-full-potential-of-artificial-intelligence.

Sambamurthy, V., and Zmud, R. W. (1999). Arrangements for Information Technology Governance: A Theory of Multiple Contingencies. MIS Quarterly, 23(2), 261-291.

Schneider, J., Abraham, R., & Meske, C. (2020). AI Governance for Businesses. arXiv preprint arXiv:2011.10672.

Sridhar, V., Subramanian, S., Arteaga, D., Sundararaman, S., Roselli, D., & Talagala, N. (2018). Model governance: Reducing the anarchy of production ML. In 2018 USENIX Annual Technical Conference (pp. 351-358).

Smith, R. (2003) The chief technology officer: strategic responsibilities and relationship. Research Technology Management, 46, 4, 28-36.

Teradata, T (2020). Teradata State of artificial intelligence for enterprises. Retrieved from https://assets.teradata.com/resourceCenter/downloads/ExecutiveBriefs/EB9867_State_of_Artificial_Intelligence_for_the_Enterprises.pdf

Trunk, A., Birkel, H., Hartmann, E. (2020). On the current state of combining human and artificial intelligence for strategic organizational decision making. Business Research, 13(1), 1-45.

Tumbas, S., Berente, N., and vom Brocke, J. (2017). Three Types of Chief Digital Officers and the Reasons Organizations Adopt the Role. MIS Quarterly Executive, 16(2), 121–134.

Utne, I. B., Hokstad, P., Vatn, J. (2011). A method for risk modeling of interdependencies in critical infrastructures. Reliability Engineering & System Safety, 96(6), 671-678.

Van den Berg, A., Struwig, M. (2017). Guidelines for Researchers Using an Adapted Consensual Qualitative Research Approach in Management Research. Electronic Journal of Business Research Methods, 15, 109-119.

Watson, G. J., Desouza, K. C., Ribiere, V. M., Lindič, J. (2021). Will AI ever sit at the C-suite table? The future of senior leadership. Business Horizons, 64(4), 465-474.

Weill, P. (2004). Don't Just Lead Govern: How Top-Performing Firms Govern IT. MIS Quarterly Executive, 3(1), 1-17.

Weill, P., and Woerner, S. L. (2013). The Future of the CIO in a Digital Economy. MIS Quarterly Executive 12(2), 65–75

Werner, F., Basalla, M., Schneider, J., Hays, D., & Vom Brocke, J. (2021). Blockchain adoption from an interorganizational systems perspective–a mixed-methods approach. Information Systems Management, 38(2), 135-150.

Whittaker, M., Crawford, K., Dobbe, R., Fried, G., Kaziunas, E., Mathur, V., … Schwartz, O. (2018). AI Now Report 2018. AI Now Institute. Retrieved from https://ainowinstitute.org/AI_Now_2018_Report.pdf

Wolfswinkel, J. F., Furtmueller, E., & Wilderom, C. P. M. (2013). Using grounded theory as a method for rigorously reviewing literature. European Journal of Information Systems, 22(1), 45–55.

Zerfass, A., Hagelstein, J., Tench, R. (2020). Artificial intelligence in communication management: a cross-national study on adoption and knowledge, impact, challenges and risks. Journal of Communication Management