Managing cyber risks in tech-oriented companies: Introducing the Three Lines Bridge Model

Duin, Esther van

Managing cyber risks in tech-oriented companies: introducing the Three Lines Bridge Model

Elisabeth Esther Maria van Duin,

Leiden University, 2448815

Contents

Word of thanks

'When we lift each other up, we all rise' – Michelle Obama

Over the last years many people have shared their knowledge with me and supported me on my journey to learn about cybersecurity and digital risks.

This thesis came to be because a lot of people wanted to contribute to my research, and helped me along the way. Not only in the form of excellent and uplifting conversations with experts, but also by the care of my friends and family. Many pot-roasts were shared with me during late nights studying, which were appreciated!

I would like to specifically thank my thesis supervisor, Tommy, who was always there when I got stuck, to discuss the questions that arose along the way, and Cristina from Leiden University for her support.

A big thank you to my employer Insulet, and to all the colleagues who stood behind me in my journey, especially to Bas.

I would also like to call out to all the people that took time to share their insights with me by participating in my research.

And of course, a special thanks to my doggo Nessie, who came to fetch me when it was time to stop studying, clear my head and take a walk outside.

1. Introduction

This thesis focuses on the way organizations professionalize their way of dealing with risks in the digital domain. More and more organizations structure their management of cyber and digital risks by applying the Three Lines Model, or some older or informal version it. We also see that when applying this model in larger tech oriented organizations, especially the traditional version where first and second lines are separated, these organizations are met with specific difficulties. Solutions to these difficulties often involve including second line knowledge into the first line, an approach that is recognized by many of the interviewees in this thesis. This thesis investigates this type of solutions as shown in the interviews, and introduces a new version of the three lines model: the Three Lines Bridge Model.

Today, regulators are facing an environment where continuous technological changes are part of every day reality. This rapid development of technology shapes a constantly changing society.[1] As lawmakers aim to establish robust, sustainable laws that will remain relevant in this fast changing environment, new approaches to legislation are introduced, for instance by using regulatory sandboxes[2] introducing more technological neutral language, and risk based approaches.[3]

As a consequence, tech-focused organisations have to deal not only with the changing technological landscape that they operate in, but also face a reality in which they have to find an effective and efficient way to implement and comply with these different types of laws, and have to deal with a more an more complex reality around risk management. In the interviews held for this thesis it became clear that tech-oriented companies are struggling to effectively manage cyber risks while faced with new laws and regulations and changing technology.

Cybersecurity is growing. Not only are the costs from attacks rising higher than ever, the industry itself is increasingly attracting more significant funding too. With global cybercrime cost estimations of over 9 trillion US dollar in 2024, the stakes are high for companies.[4] In 2025, it is estimated that revenue in the cybersecurity industry will reach approximately 203 billion US dollar.[5] As the industry is maturing, so are the company structures around this.

More and more often, cyber risk management follows a 'Three Lines', or 'Three Lines of Defense', model for risk management. This model originates from the financial industry, and was formalized in 2013 by the Institute of Internal Auditors (IIA).[6] In its initial adoption paper, the Institute of Internal Auditors state that the Three Lines of Defence Model can be used in any

[1] Taeihagh, A., Ramesh, M., & Howlett, M. (2021). Assessing the regulatory challenges of emerging disruptive technologies. *Regulation & Governance, 15*(4), 1-2.
[2] Johnson, W. G. (2022). Caught in quicksand? Compliance and legitimacy challenges in using regulatory sandboxes to manage emerging technologies. *Regulation & Governance*.
[3] Gellert, R. (2020). The risk-based approach to data protection. In *Oxford Data Protection & Privacy Law* (online edn). Oxford Academic. https://doi.org/10.1093/oso/9780198837718.001.0001
[4] Secureworks. (2024). Boardroom cybersecurity report 2024. Retrieved January 17, 2025, from https://www.secureworks.com/centers/boardroom-cybersecurity-report-2024
[5] Statista. (2024). Cybersecurity worldwide. Retrieved January 17, 2025, from https://www.statista.com/outlook/tmo/cybersecurity/worldwide
[6] The Institute of Internal Auditors. (2013). *The three lines of defense in effective risk management and control*. The Institute of Internal Auditors. Available at: https://theiia.fi/wp-content/uploads/2017/01/pp-the-three-lines-of-defense-in-effective-risk-management-and-control.pdf

organization,[7] and - perhaps unsurprisingly after such a recommendation - we see that this model is gaining popularity in managing compliance in the digital or cybersecurity domain.[8]

There are however some disadvantages for the application of this model in tech-oriented companies. In this thesis we propose an adjusted version of the Three Lines Model, in order to overcome these disadvantages and make the model better applicable to the challenges tech-focused companies face in the field of cyber risk management.

1.1 Approach to cover the new challenges

In companies with a large focus on technology a more combined effort between first- and second line employees can be observed in their approach to digital compliance and cyber risk management. This approach helps overcome some of the disadvantages of the traditional three tier model, making it a suitable method for sustainable cyber risk management as observed by privacy expert Lokke Moerel. In her paper 'Why this risk management best practice is not fit for digital innovation', she highlights the importance of integration of compliance experts in innovation teams, and the sharing of responsibility.[9]

The observed approach, with an increasingly tight knit collaboration between the first and second line, differs from the traditional Three Lines of Defense Model, where roles are more clearly defined and separated.[10] And although the revised Three Lines Model from the Institute of Internal Auditors describes possible integration between the first and second line, it does not specify what this most ideally would look like.[11]

This thesis investigates the approach to digital compliance and cyber risk management as used in companies with a strong focus on new technology, to better understand if a closer collaboration between the first and second line will lead to better risk management in these organizations. It also investigates what factors make the Three Lines Model approach successful. Building on this Three Lines Model, it introduces a modified version of it, as described by the interviewees. In order to distinguish this adjusted version from the traditional Three Lines Model, this thesis calls the adjusted version the Three Lines Bridge Model. In this Model, second line knowledge is included into the first line, thus overcoming disadvantages of the existing model in tech-oriented companies.

1.2 Research question

The research question of this thesis therefore is as follows:

Can an approach where the traditional second line knowledge is brought into the first line lead to more effective management of cyber risks, and if yes, what elements are crucial for this approach to be successful?

---

[7] The Institute of Internal Auditors. (2013). *The three lines of defense in effective risk management and control*. The Institute of Internal Auditors. Available at: https://theiia.fi/wp-content/uploads/2017/01/pp-the-three-lines-of-defense-in-effective-risk-management-and-control.pdf

[8] Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. *International Journal of Accounting Information Systems, 44*, 100548. https://doi.org/10.1016/j.accinf.2021.100548

[9] Moerel, L. (2020). Why this risk management best practice is not fit for digital innovation. Web publication/site, *IAPP*. https://iapp.org/news/a/why-this-risk-management-best-practice-is-not-fit-for-digital-innovation/

[10] Luburić, R. (2017). Strengthening the three lines of defence in terms of more efficient operational risk management in central banks. *Journal of Central Banking Theory and Practice, 6*(1), 29–53. https://doi.org/10.1515/jcbtp-2017-0003

[11] The Institute of Internal Auditors. (2020). *The IIA's three lines model: An update of the three lines of defense*. The Institute of Internal Auditors. https://www.theiia.org/globalassets/site/communication/2020/three-lines-model-updated.pdf

This research question will be addressed by answering the following sub questions, before concluding with overarching observations.

a) What are the disadvantages of the traditional three lines approach for companies with a focus on technology?
b) What are the advantages and disadvantages of consolidating the second line knowledge in the first line?
c) What are the key factors of success when implementing the Three Lines Model in large organizations with a strong focus on technology?

By answering these questions and providing overarching conclusions, this thesis aims to contribute to more effective organization structures around cyber risk management, and eventually lead to structural enhancements of newly developed technology by effectively limiting risks and meeting legal requirements.

In this first chapter an introduction of the topic is provided, and the relevance of the research and research question are addressed. The second chapter looks at what cyber risk entails. This chapter is built on existing literature, and sets the definitions on risk, cyber space and cyber risk as used in this thesis. The third chapter outlines a model aiming to structure managing risks in organizations, the Three Lines Model, and its predecessor the Three Lines of Defense Model. It explains how this model, and informal versions of it, is gaining popularity in the cybersecurity domain. The third chapter also looks at benefits and critique on the Three Lines Model as found in existing literature. Chapter four describes the method that is used in this research, which is based on semi structured interviews. This chapter includes answers to the question why this method was chosen plus a description of the interview participants, and an overview of the interviews. Chapter five to seven describe the input provided by the research participants, and how they look at effective cyber risk management in the Three Lines Model.
First, the fifth chapter looks at the disadvantages as seen by the interview participants in the Three Lines Model when used in the cybersecurity domain. Four points that are raised and discussed here are: (1) lack in quality communication between lines, (2) difficulties in creating accurate advice due to fast pace of technology and new laws, (3) limited ownership in the first line and fear of cyber risks, and (4) long turnaround time cyber risk process.
Chapter six addresses the advantages and disadvantages of including second line knowledge into the first line, as mentioned by the interviewees. This chapter also describes the importance of including second line knowledge into the first line, introducing a hybrid version of the Three Lines Model, named the Three Lines Bridge Model, with knowledge of both the first and second line into one specific role.
In the seventh chapter key factors of success for using the Three Lines Model in the cybersecurity domain are named, as described in the interviews. These include six topics: support from top management, education, contact and collaboration between teams, organizational structures, ownership and transparency and digitization.
Following the input from chapter five to seven, chapter eight then provides an analysis of the information collected during the research as described in the previous chapters. It also lists the inevitable limitations of this research and it describes proposed areas for further research. Lastly, in chapter nine the conclusion to the main research question can be found.

2. What is cyber risk?

For a clear understanding of what 'effective cyber risk management' is, it is important to first define what cyber risk management is. In this chapter the term risk is described, followed by a deeper dive into the specifics of cyber risk, and of cyber risk management. It is furthermore indicated why a broad definition of cyber risk management is applied in this thesis.

2.1 What is risk?

Close your eyes and imagine you are standing on the side of a busy road, waiting for a red light to finally turn green. You are quite hungry and you want to cross this road, as you can see your favorite bakery closing up on the other side of the street. But you do not want to get hit by any traffic.
What do you do?
You likely look at the traffic and see if there is a moment when it slows down and you can get to the other side unharmed. Maybe you consider that the cars are driving slowly, and you jump into the traffic expecting the cars to slow down for you. Or you might see only bikes, and you know that when you run into a bike the damage won't be as big as when hitting a car. Or maybe, if there is no chance to reach the other side unharmed before the traffic light changes, you wait until the green light before you proceed.

Regardless of your final decision, you have just completed a small risk assessment. As avoiding risks is in the nature of all humans,[12] you took a moment and considered the chances of getting harmed while crossing the road, taking into account the specific context of your situation such as the speed of the cars and how busy the road was at that specific time. You also reflected on the impact of your decision in case you would be hit by traffic: will it be cars or bikes that you collide with?

Risk has been defined many times in history. In 1662 Antoine Arnaud described risk as follows: '*fear of harm ought to be proportional not merely to the gravity of the harm, but also to the probability of the event*'.[13] Another more recent and almost poetic way of describing risk is provided by Heinz-Peter Berg: '*risk refers to the uncertainty that surrounds future events and outcomes.*'[14]
The first description by Arnoud, at its core identifies risk as a negative outcome or consequence (harm), taking into account the likelihood that that outcome materializes (probability of the event). Although later risk definitions were created with much more complexity, including complete mathematic formulas, the core of their descriptions usually contains a reference to a potential harm, combined with the likelihood of that harm materializing.[15] The second

[12] Ale, B. (2009). *Risk: An Introduction: The Concepts of Risk, Danger and Chance* (1st ed.). Routledge. https://doi.org/10.4324/9780203879122 chapter 1
[13] Arnaud, A. (1662). *La Logique ou l'art de penser*, p467.
[14] Berg, H.-P. (2010). Risk management: Procedures, methods and experiences. *Reliability: Theory & Application, 1*(17), 80-81.
[15] Ale, B. (2009). *Risk: An Introduction: The Concepts of Risk, Danger and Chance* (1st ed.). Routledge. https://doi.org/10.4324/9780203879122 chapter 1

description of risk by Berg does not specify the negative outcome, and focuses on the uncertainty surrounding future events. The outcome can be negative, positive or neutral. This focus on the uncertainty of a future event, be it negative, positive or neutral is another important aspect that you find back in risk definitions used today.[16] In this thesis the initial definition of Arnaud will be used where risk is identified as a possible negative outcome. This is for practical reasons, as the concept of risk used by the people included in the interviews, has a focus of possible negative outcomes, and generally disregards possible positive outcomes as risks. This may not come as too big a surprise, as within the cybersecurity community the term risks is generally only used to indicate a negative possibility, contrary to for example in the investment industry where risk can also indicate something positive.[17]

Risk management contains various steps. Firstly, the context and goals of the organization have to be established. Then, the risk has to be identified. Subsequently, the risk analysis is conducted, where consequences and probabilities are assessed, controls are established and risk prioritization is done. Then the risk evaluation takes place. Here the risk is placed against the company risk matrix, to establish if a risk is considered acceptable or not. After this step, if the risk is deemed unacceptable, it is to be remedied. After the risk has been treated, it will be monitored, to identify if the risk still exists or if the context around the risk changes, and finally information about the risk needs to be communicated, and clear risk reports are to be generated.[18]

It is interesting to pay some attention to the theory of living in a risk society, and the type of risks that are identified there since this -to some extend- describes and explains the reality of today where large organizations operate in and manage risk. Although this theory has been criticized[19] it provides context on the risk management environment in which the interviewees operate, and it shows the broader movement in which to place the findings from the research in this thesis.

In a risk society, the focus is no longer placed mainly on economic growth and technological development, which was the case in the industrial era, but instead is placed on managing risks impacting our society. Although we have become better at managing our environment, risks have become more unpredictable and more global in nature. The risks in the so called risk society are often the consequence of human action, even though the specific risk is not always clear at the moment of the action. However, as barely any domains remain in which humans are not involved, the odds are that human actions will almost always contribute to. at times unknown, risks down the line.[20] In this risk society, there are two types of risk present: external risk, and manufactured risk. External risks relate to unexpected but regularly occurring risks, such as floods, or illnesses. Manufactured risks are less predictable and come from uncertainties from human actions such as technological developments. Think about the

[16] Berg, H.-P. (2010). Risk management: Procedures, methods and experiences. *Reliability: Theory & Application, 1*(17), 80-81.
[17] Bayuk, J. L. (2024). *Stepping through cybersecurity risk management: A systems thinking approach*. Wiley. https://doi.org/10.1002/9781394213986
[18] Berg, H.-P. (2010). Risk management: Procedures, methods and experiences. *Reliability: Theory & Application, 1*(17), 82-92.
[19] See for example: Adam, B., Beck, U., & Van Loon, J. (2000). *The risk society and beyond: Critical issues for social theory*. SAGE Publications Ltd.
[20] Giddens, A. (1999), Risk and Responsibility. *The Modern Law Review, 62,* p1-5 https://doiorg.ezproxy.leidenuniv.nl/10.1111/1468-2230.00188.

creation of nuclear waste, or other risks in new environments where we cannot predict what will happen in the future.[21] Both types of risk are relevant as they play an important role in cyber risk. Next to that, the latter specifically is a risk that is difficult to mitigate in tech-oriented companies, since these companies are strongly interacting with new environments where possible unknown risks in cyber space can arise, with which risk professionals need to deal. An important part of a risk society is that the amount of attention drawn to risks in part identifies the perceived importance of the risk. At the same time the possibility exists that a risk does not materialize, which can lead to the person identifying the risk being portrayed as 'someone who cried wolf'. This might work as a deterrent and makes it difficult to ensure that risk management is objective. This struggle is something you see for example in politics, but also in risk mitigation and ownership conversations in organizations.

2.2 What is cyber risk?

The threat of cyber risk is one that is increasingly gaining attention.[22] As mentioned in the above section about risk, this thesis uses a risk definition similar to the one described by Arnaud, focusing on harms or negative outcomes. As a consequence, when considering cyber risk this thesis will focus on possible harm in cyberspace and leave out the possibility of positive consequences.

Literature about cyber risk varies in their approach and scope of what falls under the definition. There are authors who approach cyber risk with a narrow focus, looking at operational IT risks impacting confidentiality, integrity or availability of information and assets only.[23] [24] These definitions, although the term 'cyber risk' is used, often refer to definitions provided for cybersecurity risk specifically, for example the one provided by James Cebula and Lisa Young in '*A Taxonomy of Operational Cyber Security Risks*'.[25] Interestingly enough, even in the cybersecurity domain there are variations when addressing the scope of cybersecurity risk, where recent authors apply a broader approach to security risk, including legal, reputational or regulatory consequences to their approach.[26]

For this thesis the focus of cyber risk is aimed beyond the narrow scope, and beyond focusing only on cyber security risk. Instead it build on a broader approach to cyber risk. To establish this broader approach, a closer look at the meaning of the term 'cyber' is needed. As cyber refers to cyber space, cyber risk should relate to risk within this cyber space domain.[27] As a next step, we need to identify what the digital domain or cyberspace entails. For this, the thesis follows the explanation used in the Cyber Harm Model. In this model, cyber space is considered a

---

[21] Giddens, A. (1999), Risk and Responsibility. *The Modern Law Review, 62,* p1-5 https://doiorg.ezproxy.leidenuniv.nl/10.1111/1468-2230.00188.

[22] Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2022). *The drivers of cyber risk. Journal of Financial Stability, 60,* 100989-. https://doi.org/10.1016/j.jfs.2022.100989

[23] Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. *The Geneva Papers on Risk and Insurance - Issues and Practice, 47*(3), 698-736. https://doi.org/10.1057/s41288-022-00266-6[1](https://link.springer.com/article/10.1057/s41288-022-00266-6).

[24] Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of Cyber Risk: An Empirical Analysis. *Geneva Papers on Risk and Insurance. Issues and Practice, 40(1),* 131–158. https://doi.org/10.1057/gpp.2014.19

[25] Cebula, J. L., & Young, L. R. (2010). *A Taxonomy of Operational Cyber Security Risks*.

[26] Allen, B. J., & Loyear, R. (2018). *Enterprise security risk management: concepts and applications* (K. Noakes-Fry, Ed.; 1st ed.). Rothstein Publishing. Chapter 3.

[27] Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of Cyber Risk: An Empirical Analysis. *Geneva Papers on Risk and Insurance. Issues and Practice, 40(1),* 132–134. https://doi.org/10.1057/gpp.2014.19

combination of the physical infrastructure creating the cyberspace, and the way this physical environment is used. Cyberspace is divided into six elements: an ecosystem, built by digital technologies, connected through networks, where various actors show different behaviors regarding the creation, storage, modification, sharing and exploitation of information, treating cyberspace as an operational space.[28] This fits with the risks in a company setting, where there are both risks relating to the physical cyber infrastructure itself (e.g., the network cables are cut), as well as to the use of the physical network that builds cyber space (e.g., malicious actors leaking company data).

Following the above, cyber risk is therefore referred to as the possible negative outcome of a situation in the digital domain or cyber space, while considering the likelihood of the negative outcome to becoming reality. This aligns with commonly used terminology of cyber risk,[29] or as others have described it in the past as E-risk.[30]

As part of this broad approach, negative outcomes for companies from not complying with relevant regulatory requirements in the digital domain are also included. This means that possible fines, or at times even legal action towards individual stakeholders in an organization are part of the definition of cyber risk, if they are the (indirect) consequence of an action or negligence from actors in cyberspace. It becomes even more relevant to include risks from new laws and regulations in the digital domain into cyber risk, as globally an increasing number of laws appear to regulate the digital domain.[31] It is a challenge for legislators worldwide to cope with regulating new technologies and their unknown consequences, as currently existing tools are often insufficient. And as they are struggling, companies trying to adhere to relevant laws and regulations regarding this domain struggle with compliance.

This approach also means that in addition to information security risks, other risk domains such as data protection risk, IT risk and AI risk also (partially) fall under the definition of cyber risk.

2.3 What is cyber risk management?

One way of explaining risk management is to use information from the past in order to predict what will happen in the future.[32] Cyber risk management builds on this explanation, as well as on the definition of cyber risk, and can be defined as: identifying possible negative outcomes in the cyber or digital environment, and determining ways to prevent these harms from materializing.[33]

---

[28] Berg, B. van den, & Kuipers, S. L. (2022). Vulnerabilities and cyberspace: A new kind of crisis. *Oxford Research Encyclopedia of Politics*. https://doi.org/10.1093/acrefore/9780190228637.013.1604.

[29] Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2022). The drivers of cyber risk. *Journal of Financial Stability, 60*, 100989. https://doi.org/10.1016/j.jfs.2022.100989

[30] Mukhopadhyay, Arunabha & Saha, Debashis & Mahanti, Anirban & B, Chakrabarti & A, Podder. (2005). Insurance for Cyber-risk: A Utility Model. Decision. 32. P156-157.

[31] See for example the Europe Fit for the Digital Age initiative in the EU. European Commission. Europe fit for the digital age. Retrieved from https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en

[32] Bayuk, J. L. (2024). *Stepping through cybersecurity risk management: A systems thinking approach*. Wiley. https://doi.org/10.1002/9781394213986

[33] Brumfield, C. (2022). *Cybersecurity risk management: Mastering the fundamentals using the NIST cybersecurity framework*. John Wiley & Sons, Inc. https://doi.org/10.1002/9781119816348

There are many ways and frameworks to manage cyber risk,[34] often following a similar pattern as discussed in section 2.1: establishing context, identifying risks, performing a risk analysis and a risk evaluation, and if needed the risk is treated and afterwards monitored. Lastly risks are communicated.[35]
A popular model for security risk management involves the US National Institute of Standards and Technology (NIST) Cybersecurity framework, on which the European Union based its first Cybersecurity Directive.[36] This Cybersecurity Directive, or NIS Directive[37] has now been updated into the NIS2 Directive.[38] Many bigger organizations have implemented this NIST framework, and research in 2016 showed that out of 338 IT professionals that were interviewed, 70% considered it a best practice.[39]

The NIST Cybersecurity framework, which was updated in 2024 to a 2.0 version, includes various functions to facilitate cyber security risk management, which can also be used when addressing broader cyber risks. These steps include: Govern, Identify, Protect, Detect, Respond, and Recover. The function 'Govern' did not exist until the latest update of the NIST framework, in which the function was added. This function ensures there is a cyber risk strategy, and furthermore it creates, monitors and communicates policies and sets prioritization of the other functions within cyber risk management.[40] This aligns with the step in general risk management that looks at establishing the risk context. The fact that this is newly included in the frequently used NIST cybersecurity framework emphasizes the need for a more specific defined cyber risk governance.

Cyber risk management is de facto a process that manages how to deal with possible negative outcomes in the cyber domain. In the functions of the NIST framework various steps are included, such as framing risks, assessing risks, responding to risks and risk monitoring. In addition, the framework requires roles and responsibilities to be established and implemented.[41] Other approaches, such as the Enterprise Security Risk Management life cycle, use similar underlying principles.[42]

[34] This immediately shows a difficulty for cyber risk management, considering that the cyber environment is still relatively young and keeps changing.
[35] Berg, H.-P. (2010). Risk management: procedures, methods and experiences. *Reliability: Theory & Application 1(*17): 82-92.
[36] Krumay, B., Bernroider, E. W. N., Walser, R., & Gruschka, N. (2018). Evaluation of cybersecurity management controls and metrics of critical infrastructures: A literature review considering the NIST cybersecurity framework. In *Secure IT Systems* (Vol. 11252, p. 369–384). Springer International Publishing AG. https://doi.org/10.1007/978-3-030-03638-6_23
[37] European Union. (2016). *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*. Official Journal of the European Union, L 194, 1-30
[38] European Union. (2022). *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)*. Official Journal of the European Union, L 333, 80-152.
[39] Krumay, B., Bernroider, E. W. N., Walser, R., & Gruschka, N. (2018). Evaluation of cybersecurity management controls and metrics of critical infrastructures: A literature review considering the NIST cybersecurity framework. In *Secure IT Systems* (Vol. 11252). Springer International Publishing AG. https://doi.org/10.1007/978-3-030-03638-6_23
[40] National Institute of Standards and Technology. *NIST Cybersecurity Framework (CSF) 2.0*. https://doi.org/10.6028/NIST.CSWP.29
[41] Brumfield, C. (2022). *Cybersecurity risk management: mastering the fundamentals using the NIST cybersecurity framework*. John Wiley & Sons, Inc. https://doi.org/10.1002/9781119816348 p3-4.
[42] Allen, B. J., & Loyear, R. (2018). *Enterprise security risk management: concepts and applications* (K. Noakes-Fry, Ed.; 1st ed.). Rothstein Publishing. Chapter 5.

An important part of cyber risk management revolves around asset management.[43] Having an overview of what applications and systems are running is crucial to understand the risks that may live within an organization. This includes a rating of the importance of the applications, updates to the list and ensuring sufficient skilled workers are contracted to review and maintain the inventory.[44] In addition to creating and maintaining an inventory, cyber risk management includes having a strong governance around cyber risk. This means it is crucial to have appropriate policies and procedures in place, documenting which actions to take to protect the organization from cyber harm, and reviewing if the policies and documented actions are executed continuously. Having a strong governance also requires training and awareness activities, to ensure that employees are aware of cyber risks, and that management organizations can take appropriate actions, particularly considering that the higher management is being increasingly held accountable personally for cyber incidents. It also includes ensuring an organization understands laws and regulations and how to comply.[45]
A third part of cyber risk management revolves around what people traditionally think of first, when asked what cyber risk management entails: the part where cyber risk assessments are performed, and where risks are mitigated. This means organizations need to understand where their vulnerabilities lie, what threats they face, and what possible risks are. Questions asked in this part include if there are physical risks to an asset, if the asset is a likely target for cybercrime operations, and whether there are regulatory requirements that need to be met.[46] Organizations also need to determine what to prioritize regarding risks, which is likely impacted by what is deemed important. For this step it is crucial to build on the asset inventory, and to involve stakeholders from different parts of the organizations depending on their relation to the risk.[47] Once these actions are undertaken, (high) risk mitigations are created and subsequently executed. The step of performing cyber risk assessments and mitigations is repeated on a regular basis as vulnerabilities, threats and the focus of the organization can change over time. Risk assessments are dependent on clear allocation of ownership for business processes and assets. Subsequently, cyber risks must be allocated to the respective process- or asset owners, who are accountable for executing the mitigations (or acceptance) of risks.[48]

In conclusion, cyber risk management is the process in which we aim to organize possible cyber risks to limit possible negative outcomes.

3. What is the Three Lines Model?

In both literature and everyday life, discussions regarding organizations involving a risk context often reference the Three Lines of Defense Model and its successor the Three Lines Model -a

[43] Allen, B. J., & Loyear, R. (2018). *Enterprise security risk management: concepts and applications* (K. Noakes-Fry, Ed.; 1st ed.). Rothstein Publishing. Chapter 5.
[44] Brumfield, C. (2022). *Cybersecurity risk management: mastering the fundamentals using the NIST cybersecurity framework*. John Wiley & Sons, Inc. https://doi.org/10.1002/9781119816348 p.4-13.
[45] Brumfield, C. (2022). *Cybersecurity risk management: mastering the fundamentals using the NIST cybersecurity framework*. John Wiley & Sons, Inc. https://doi.org/10.1002/9781119816348 p13-14.
[46] Allen, B. J., & Loyear, R. (2018). *Enterprise security risk management: concepts and applications* (K. Noakes-Fry, Ed.; 1st ed.). Rothstein Publishing. Chapter 5
[47] Allen, B. J., & Loyear, R. (2018). *Enterprise security risk management: concepts and applications* (K. Noakes-Fry, Ed.; 1st ed.). Rothstein Publishing. Chapter 5.
[48] Brumfield, C. (2022). *Cybersecurity risk management: mastering the fundamentals using the NIST cybersecurity framework*. John Wiley & Sons, Inc. https://doi.org/10.1002/9781119816348 p15-20.

modified version of the former model. As such, before analyzing the advantages or disadvantages, let's take a closer look at what this model entails, according to existing literature.

3.1 The Three Lines of Defense Model

Although versions of the model had been around for a while, with different theories around its origin,[49] two important institutions are often named regarding the introduction of what we know as the Three Lines of Defense Model: the Basel Committee of Banking Supervision[50] and the Institute of Internal Auditors.[51] In their initial description of the model the first line of defense works on creating a product or a service. This line also owns risks. The second line reviews the work done by the first line and provides advice to ensure compliance with relevant laws and regulations. The second line also creates risk frameworks and identifies risks where needed. The third line entails an independent function in the organization and has the responsibility to audit the work of the first and second line.[52]

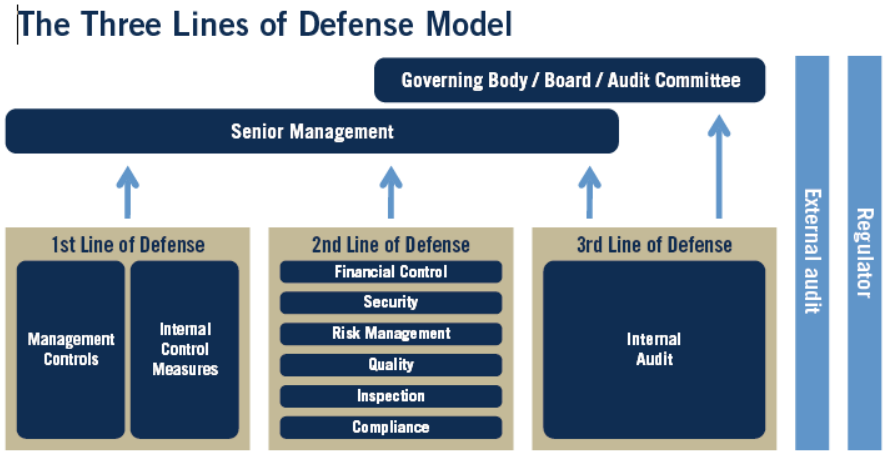

Fig 1. The Three Lines of Defense Model (TLM) as published by IIA in 2013 [53]

The Three Lines of Defense Model aims, as is in the name, to defend against risks, and to do so in a structural manner. The Institute of Internal Auditors addresses the challenge to assign specific roles and coordinate between them, preventing gaps in controls.[54] It mentions issues

[49] Schuett, J. (2023). Three lines of defense against risks from AI. *AI & Society*. https://doi.org/10.1007/s00146-023-01811-0
[50] Basel Committee on Banking Supervision, Bank for International Settlements. (2011). *Principles for the sound management of operational risk*. https://www.bis.org/publ/bcbs195.pdf and
Basel Committee on Banking Supervision, Bank for International Settlements. (2014). *Review of the principles for the sound management of operational risk*. https://www.bis.org/publ/bcbs292.pdf
[51] The Institute of Internal Auditors. (2013). *The three lines of defense in effective risk management and control*. The Institute of Internal Auditors. Available at: https://theiia.fi/wp-content/uploads/2017/01/pp-the-three-lines-of-defense-in-effective-risk-management-and-control.pdf
[52] Luburić, R. (2017). Strengthening the three lines of defence in terms of more efficient operational risk management in central banks. *Journal of Central Banking Theory and Practice,* 6(1), 29–53. https://doi.org/10.1515/jcbtp-2017-0003 and
Schuett, J. (2023). Three lines of defense against risks from AI. *AI & Society*. https://doi.org/10.1007/s00146-023-01811-0
[53] The Institute of Internal Auditors. (2013). *The three lines of defense in effective risk management and control*. The Institute of Internal Auditors. Available at: https://theiia.fi/wp-content/uploads/2017/01/pp-the-three-lines-of-defense-in-effective-risk-management-and-control.pdf
[54] The Institute of Internal Auditors. (2013). *The three lines of defense in effective risk management and control*. The Institute of Internal Auditors. Available at: https://theiia.fi/wp-content/uploads/2017/01/pp-the-three-lines-of-defense-in-effective-risk-management-and-control.pdf

when no enterprise risk management framework is used, which can lead to situations where conversations about risks are limited to the subject of task assignments.

When in 2007 and 2008 the financial crisis hit the globe, and it became apparent that failure of risk management played a partial role, the demand for a structured approach to enterprise risk management increased.[55] As a consequence, the Three Lines of Defense Model became a new standard for risk management. A 2015 survey conducted amongst internal audit professionals from 166 countries, with over 14000 participants, showed that over 75% of the respondents indicated to use the model in their organization.[56] Although big tech companies seem underrepresented in the results of the 2015 survey in using the model, it has been gaining popularity in the cybersecurity domain.[57]

3.2 The Three Lines Model

Following their publication of the Three Lines of Defense model in 2013, the Internal Institute of Auditors has updated its take on the model, and published a new version in 2020. This new version is named the Three Lines Model. In this version, the Institute of Internal Auditors included several additional principles and roles, such as external assurance, governance bodies, and the role of management. The governance bodies have various tasks, such as accountability for organizational oversight, ensuring a culture of ethical behavior, determining the risk appetite of the organization, and overseeing the third line, which is the independent audit function. It also shifted its focus way from only defense, and acknowledged that risk need to be taken and managed to create value.[58]

The added management function in this new version of the model coordinates the first and second line. The first and second line here are similar to the lines as mentioned above in the description of the original Three Lines of Defense Model. The first line creates products and services, manages risks, aligns with the governing body, and complies with expectations and guidance set by the second line. The second line does not set the risk appetite, as this is done by the governance bodies, but it supports, monitors and challenges the first line in its risk management actions, provides risk management tools and controls, sets the objectives of risk management and advices on compliance with laws and regulations. This second line also reports on the effectiveness of risk management within the organization.[59] In the revised Three Lines Model, the Institute of Internal Auditors also provides an updated view on how the first and second line should work together compared to the traditional Three Lines of Defense model. In this version, supported by a more recent opinion paper in September 2024,[60] it is described how the first and second line do not have to be completely separated, but if preferred

[55] Schuett, J. (2023). Three lines of defense against risks from AI. *AI & Society*. https://doi.org/10.1007/s00146-023-01811-0

[56] Huibers, S. C. J. (2015). *Combined assurance: One language, one voice, one view*. The Institute of Internal Auditors Research Foundation. Available at: https://perma.cc/D7YM-9GS

[57] Valkenburg, B., & Bongiovanni, I. (2024). Unravelling the three lines model in cybersecurity: a systematic literature review. *Computers & Security*, *139*, 103708-. https://doi.org/10.1016/j.cose.2024.103708

[58] Slapničar, S., Axelsen, M., Bongiovanni, I., & Stockdale, D. (2022). *A pathway model to five lines of accountability in cybersecurity governance*. University of Queensland.

[59] The Institute of Internal Auditors. (2020). *The IIA's three lines model: An update of the three lines of defense*. The Institute of Internal Auditors. https://www.theiia.org/globalassets/site/communication/2020/three-lines-model-updated.pdf

[60] The Institute of Internal Auditors. (2024). *The IIA's three lines model: An update of the three lines of defense*. The Institute of Internal Auditors. Available at: https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf

can also operate in a more blended manner.[61] This is a change in their approach compared to the initial Three Lines of Defense version from 2013.

In the Three Lines Model, the third line is similar to its original version as defined in the Three Lines of Defense Model. It is embodied in the independent internal audit function and is as such accountable to the governing body and independent from management. It reports on the overall adequacy of the risk management within the organization and provides recommendations for improvements. Furthermore, it is responsible for safeguarding the independence of the risk management function within the organization and must report any impairments regarding this independence to the governing body.[62]

The third line's assurance is complemented by the external assurance providers who verify assurance regarding regulatory requirements to protect the interest of stakeholders.

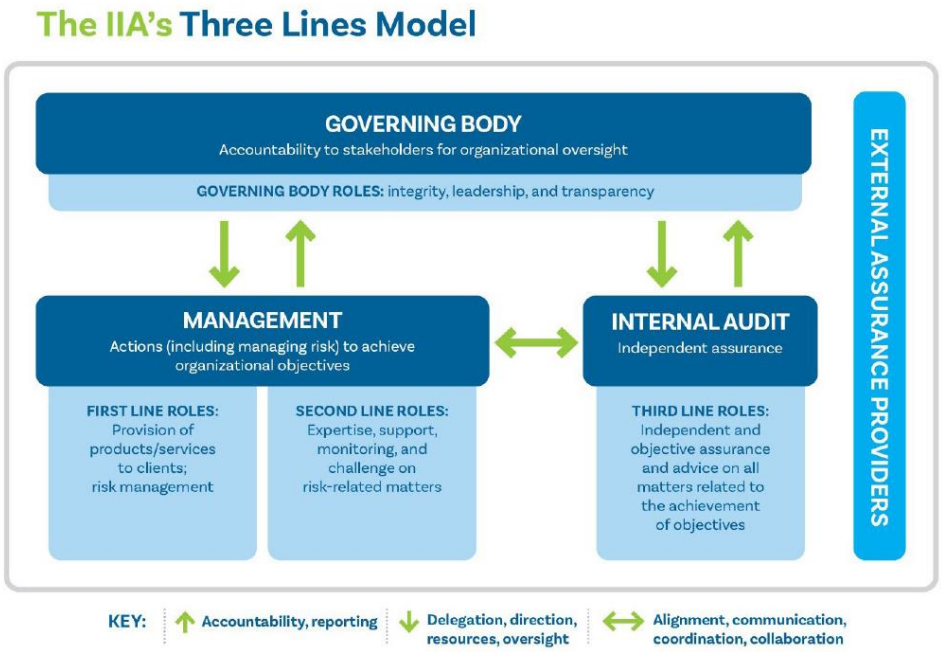

Fig 2. Updated Three Lines of Defense Model (TLM), now called the Three Lines Model.[63]

The updated model further emphasizes the importance of alignment on the organizational goals, and the need for strong collaboration and communication in order for the model to facilitate good risk management. It describes the possibility for teams and individuals in management to have first and second line responsibilities, however it recommends that direction and oversight on the second line is independent from the first line, even when reporting to the government body.

[61] The Institute of Internal Auditors. (2024). *The IIA's three lines model: An update of the three lines of defense*. The Institute of Internal Auditors. Available at: https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf

[62] The Institute of Internal Auditors. (2024). *The IIA's three lines model: An update of the three lines of defense*. The Institute of Internal Auditors. Available at: https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf and
The Institute of Internal Auditors. (2020). *The IIA's three lines model: An update of the three lines of defense*. The Institute of Internal Auditors. https://www.theiia.org/globalassets/site/communication/2020/three-lines-model-updated.pdf

[63] The Institute of Internal Auditors. (2020). *The IIA's three lines model: An update of the three lines of defense*. The Institute of Internal Auditors. https://www.theiia.org/globalassets/site/communication/2020/three-lines-model-updated.pdf

As the Three Lines Model is relatively new, there is limited research has been conducted on the effectiveness of the model, particularly in the field of cybersecurity. A first systematic literature of the model in the field of cybersecurity was published in 2024.[64] The reframing of the model by the Institute of Internal Auditors can possibly facilitate a blended model in which the first and second line work together more closely, however further research is necessary on this collaboration. This thesis provides this research, and describes a blended Three Lines Model, the Three Lines Bridge Model.

3.3 Benefits Three Lines of Defense Model and the Three Lines Model

The Three Lines of Defense model was introduced in the financial sector to facilitate an enterprise risk management oversight structure, to minimize the possibility of gaps in risk management and to limit significant failure of implemented controls.[65] The model -and later the Three Lines Models as well- ensure that different perspectives are provided to risk, and that risks are addressed systematically and not ad hoc.[66] As a result, risks are managed more effectively.[67]

The model is considered practical, both for organizations dealing with risk, as well as for regulators. In its initial principles, the Basel Committee on Banking Supervision stated that the Three Lines of Defense model often underlines good operational risk governance.[68]
It provides transparency around roles and responsibilities. At the same time, it provides a clear blueprint of how to organize and document the management of nonfinancial risks, which is beneficial when an organization needs to respond to questions from their stakeholders like regulators or the board of directors amongst others.[69]

The clarity around roles and responsibilities provided by the Three Lines Model when used in cybersecurity, can support with investments into cybersecurity and the design of the organizational structure around cybersecurity, enabling enhanced alignment of cybersecurity governance with the rest of the organizational governance.[70]

3.4 Critique Three Lines of Defense and the Three Lines Model

In addition to the benefits, the model is also met with significant criticism in academic literature. This can be attributed to the fact that the Three Lines Model is, in fact, a model, and

---

[64] Valkenburg, B., & Bongiovanni, I. (2024). Unravelling the three lines model in cybersecurity: a systematic literature review. *Computers & Security*, *139*, 103708-. https://doi.org/10.1016/j.cose.2024.103708
[65] Brender, N., Gauthier, M., Morin, J.-H., & Salihi, A. (2024). Three lines model paradigm shift: a blockchain-based control framework. *Journal of Applied Accounting Research*, *25*(1), 149–170. https://doi.org/10.1108/JAAR-06-2022-0143
[66] Seidenfuss, K.-U., Young, A., & Datwani, M. (2023). Integrating governance, risk and compliance? A multi-method analysis of the new Three Lines Model. *SN Business & Economics*, *3*(10). https://doi.org/10.1007/s43546-023-00561-x
[67] Valkenburg, B., & Bongiovanni, I. (2024). Unravelling the three lines model in cybersecurity: a systematic literature review. *Computers & Security*, *p3*, 103708-. https://doi.org/10.1016/j.cose.2024.103708
[68] Basel Committee on Banking Supervision, Bank for International Settlements. (2011). *Principles for the sound management of operational risk*. https://www.bis.org/publ/bcbs195.pdf and
Basel Committee on Banking Supervision, Bank for International Settlements. (2014). *Review of the principles for the sound management of operational risk*. https://www.bis.org/publ/bcbs292.pdf
[69] Hoefer E, Cooke M, Curry T (2020) Three lines of defense—Failed promises and what comes next. Financial regulatory Forum, 8 Sep 2020. https://www.reuters.com/article/bc-finreg-risk-management-three-lines-of-idUSKBN25Z2FN/
[70] Valkenburg, B., & Bongiovanni, I. (2024). Unravelling the three lines model in cybersecurity: a systematic literature review. *Computers & Security*, *139*, 103708-. https://doi.org/10.1016/j.cose.2024.103708

as such provides a simplification of reality.[71] Highlighted below are some of the main points of critique found in literature.

3.4.1 Lack of collaboration

Implementing segregation of duties, with an independent second line as recommended by the Three Lines of Defense Model and later the Three Lines Model,[72] leads to problems when trying to limit risks and comply with new laws and regulations focused on technology.[73] Often the second line works in isolation, despite the fact that collaboration is crucial for success.[74] The segregation of duties encourages a siloed approach of lines, making the lines inflexible, where in reality these need to be closely connected.[75] As safe and compliant technology often requires innovation and development of new features to facilitate compliance and risk minimization, it becomes clear that compliance experts are needed in the development teams themselves to work on this. This is the opposite of a situation in which the second line is placed outside the design and innovation process, as an independent function. The separation of lines does not sufficiently facilitate such close collaboration in the creation process.[76]

This critique seems reflected in the recent revisions of Three Lines of Defense Model into the new Three Lines Model, and is mentioned in a position paper published in September 2024 by the Institute of Internal Auditors. Here it is stated that the first and second line may be separated or blended,[77] deviating from the initial break down of the first and second line as described in the initial Three Lines of Defense Model.[78] This reframing of the model can possibly facilitate a blended model in which the first and second line work together more closely, however further research is necessary on this collaboration. This thesis provides this research, and describes a blended Three Lines Model, the Three Lines Bridge Model.

3.4.2 Effectiveness & Efficiency

The effectiveness and efficiency of the model is also critiqued, as the focus is mainly on preventable risks, and less so on risks with a more strategic or external element. In addition, possible misaligned incentives are named.[79] This can be when the first line has a (for real or perceived) difference in objectives from the second line. Other points of concern about the model relate to topics such as a lack of skills and lack of resources, leading to a limited effectiveness of the model. From an efficiency perspective, there is concern about duplication of work, and difficulties around scalability of the roles in the model when needed.

---

[71] Seidenfuss, K.-U., Young, A., & Datwani, M. (2023). Integrating governance, risk and compliance? A multi-method analysis of the new Three Lines Model. *SN Business & Economics*, *3*(10). P10. https://doi.org/10.1007/s43546-023-00561-x

[72] Luburić, R. (2017). Strengthening the Three Lines of Defence in Terms of More Efficient Operational Risk Management in Central Banks. Journal of Central Banking Theory and Practice (Podgorica), 6(1), 29–53. https://doi.org/10.1515/jcbtp-2017-0003

[73] Moerel, L. (2020). Why this risk management best practice is not fit for digital innovation. Web publication/site, IAPP

[74] Haelterman, H. (2020). Hard, soft or situational controls? Bridging the gap between security, compliance and internal control. SECURITY JOURNAL, 33, 636–656. https://doi.org/10.1057/s41284-019-00208-3

[75] Seidenfuss, K.-U., Young, A., & Datwani, M. (2023). Integrating governance, risk and compliance? A multi-method analysis of the new Three Lines Model. *SN Business & Economics*, *3*(10). https://doi.org/10.1007/s43546-023-00561-x

[76] Moerel, L. (2020). Why this risk management best practice is not fit for digital innovation. Web publication/site, IAPP

[77] The Institute of Internal Auditors. (2024). *The IIA's three lines model: An update of the three lines of defense*. The Institute of Internal Auditors. Available at: https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf

[78] The Institute of Internal Auditors. (2024). *The IIA's three lines model: An update of the three lines of defense*. The Institute of Internal Auditors. Available at: https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf

[79] Seidenfuss, K.-U., Young, A., & Datwani, M. (2023). Integrating governance, risk and compliance? A multi-method analysis of the new Three Lines Model. *SN Business & Economics*, *3*(10). https://doi.org/10.1007/s43546-023-00561-x

3.4.3 Keeping up the pace

Another point of critique when using the Three Lines Model for new technology relates to the (usually slow) pace of new legislation being developed as compared to the pace at which new technology is released. It is difficult for law makers to regulate new technology when it is often unclear what kind of risks may arise and which unwanted consequences may appear.[80]

When developing new technology, it is insufficient for the first line to only await input from the second line when it comes to preventing risks in new products. New technologies are frequently not (completely) regulated upfront, or there is often a certain degree of uncertainty on how new developments in technology will play out and which societal issues may need to be regulated as a result.[81] Not only will this lead to situations where regulators and law makers cannot keep up with how fast technology develops, but also to situations in which it is difficult for the second line to provide controls or company policies to the first line, especially when working in isolation from the first line.[82] The laws and regulations on which the second line bases itself when creating policies and assessing risk appetite are often not fully developed and may change. This can be illustrated by various examples of new laws and regulations, such as a new privacy law implemented in the Kingdom of Saudi Arabia, the Personal Data Protection Law (hereafter PDPL). The initial version of this law was introduced with several obligations that were either changed or removed in a later version of the law, or that required additional guidance which did not become available until much later. In this example, one of the requirements included severe restrictions on sharing data outside the Kingdom of Saudi Arabia, and an obligation for organizations to register their processing activities in a centralized government owned register, without providing any details on the register or the specific information that should be present in the registration.[83] Later, in a revised version of the law the requirement for the registration of processing activities in a national register was removed when the article regarding the national register for processing activities was repealed. In addition, the limitations to cross-border data processing were lifted.[84] A clear guidance document describing the requirements of an internal register that organizations need to maintain was only published in the course of 2024.[85]

A similar challenge can be observed when looking at new technologies, when no regulations exists yet and must still be developed. An example of this can be found in the added provisions to the European AI act regarding generative AI, after ChatGPT became extremely popular and regulators realized there was an immediate need for regulation of this new technology.[86] At times where there is no clear regulation to comply with yet, the second line cannot provide adequate guidance as there is no estimable business risk for noncompliance.

---

[80] Taeihagh, A., Ramesh, M., & Howlett, M. (2021). Assessing the regulatory challenges of emerging disruptive technologies. *Regulation & Governance, 15*(4).

[81] Johnson, W. G. (2022). Caught in quicksand? Compliance and legitimacy challenges in using regulatory sandboxes to manage emerging technologies. *Regulation & Governance*.

[82] Moerel, L. (2020). Why this risk management best practice is not fit for digital innovation. *IAPP*. https://iapp.org/news/a/why-this-risk-management-best-practice-is-not-fit-for-digital-innovation/

[83] Saudi Authority for Data and Artificial Intelligence. (2021). *Personal Data Protection Law (*Article 29 and Article 32).

[84] See Saudi Authority for Data and Artificial Intelligence. (2023). *Personal Data Protection Law (Version 2) (*Article 29 and Article 32). Retrieved from https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal%20Data%20English%20V2-23April2023-%20Reviewed-.pdf as well as explanatory articles from law firms such as: Saudi Arabia's amended Personal Data Protection Law, 7 April 2023,

[85] Saudi Authority for Data and Artificial Intelligence. *Personal Data Processing Activities Records Guideline*. Retrieved from https://sdaia.gov.sa/Documents/PersonalDataProcessingActivitiesRecordsGuideline.pdf

[86] Stibbe. (2023). *EU Artificial Intelligence Act and Generative AI: An Update*. Retrieved from https://www.stibbe.com/publications-and-insights/eu-artificial-intelligence-act-and-generative-ai-an-update

This lack of clear existing guidance upfront, next to the fact that new laws are not yet ready or additional guidance on how to interpret these laws can change on short notice, and together with the uncertainty of the regulations altering in a later stage, consequently means it is often impossible for the second line to provide clear cut guidance to the first line on what activities to undertake for compliance- and risk management purposes. In the case of the Saudi law for example, the requirement to 'register your processing activity' could not be made concrete, and the initial limitations to transfer personal data outside the Kingdom required significant technological investments for parties working there, as for instance the use of clouds outside the country would be significantly more difficult or at times not possible. For developers of AI this meant they had a brand new law to take into account, which provided uncertainty on possible new product requirements in the midst of a development boom, as the AI Act was implemented in the midst of the uptake of the use of generative AI.

4. Method description

4.1 Method used

For this thesis two methods of gaining knowledge have been applied: the study of existing literature on the subject of cyber risk management and the Three Lines Model as included in the previous chapters, and the conducting of semi structured interviews with experts in the field. This method of semi structured interviews was chosen as literature on the research topic is scarce and relatively limited. Conducting interviews with experts proved a valuable method to gain more information.

Semi structured interviews were used, to ensure that during a conversation the interview respondents could elaborate on specific crucial topics, and to ensure that questions could be skipped in case the interview respondent did not relate to a topic.

A more in-depth specification of the method is provided below.

4.2 Interviews and interview set-up

As mentioned above, semi structured interviews were conducted for this research, as there is limited literature available on cybersecurity following the Three Lines Model.

Before conducting the interviews, an outline was created for the interviews, taking into account the target group for the interviews, the interview approach and the interview questions. This resulted in an approach where 13 interviews were conducted with different experts in the field of cybersecurity, covering different roles and different knowledge and expertise on the subject as is explained below (see paragraph 4.3.2).

The following sub questions of this thesis were addressed in these interviews:

a) What are the disadvantages of the traditional three lines approach for large companies with a focus on technology?
b) What are the advantages and disadvantages of consolidating the second line knowledge in the first line?

c) What are the key factors of success when implementing the three lines model in large organizations with a strong focus on technology?

By asking these questions to relevant experts in the field, it was possible to extract information on the perceived key factors of success when organizing cyber risk management. Furthermore it gave insight in what the experts considered advantages of consolidating second line knowledge into the first line.

As a result of the information obtained from the interviews, answers were found to the overarching main question:

Can an approach where the traditional second line knowledge is brought into the first line lead to more effective management of cyber risks, and if yes, what elements are crucial for this approach to be successful?

4.2.1 Interviewees: a jury of experts

When looking for interview participants, the focus was on experts that either work in compliance related functions or business related functions, within companies with a large emphasis on technology, where there is a close collaboration between the traditional first and second line functions. An extra consideration when choosing interviewees was to aim to include participants with a track record in compliance related functions while working in the first line, or who had experienced working in second line functions whilst closely collaborating with first line employees.

Experts from the professional network of the author of this paper were approached where possible and proved to be a helpful resource, thus reducing the need for so called 'cold calling' of people. In addition, experts were contacted outside of the personal network, based on their role within tech related organizations at work related events.

The interviews mostly took place via Teams video calls, with the exception of three interviews which were conducted in person. An overview of the relevant roles and industries of all participants is provided below. The goal was to include people from different industries and different layers of the organization, both in the first and second line. The result is a mix of first- and second line experts, in different industries and on different management levels, which provided a balanced overview of input for this research.

4.2.2 Approach: generic

A generic research approach was followed, instead of researching questions specifically related to a case. Although using a predefined case would have had the benefit of directing the research outcomes more towards a specific situation, it would at the same time limit the freedom for insights outside the framework of the case. By refraining from using one or more specific cases, interviewees were provided with freedom to move conversations in for them relevant directions.

The chosen method thus allowed for a broad approach towards digital compliance and cyber risk management, which as an added benefit means it was not too difficult to find relevant research participants. Had the interviews been limited to a specific case, e.g. a privacy or AI case, experts in the field of security or data compliance could not have been included.

4.2.3 Questions

The following interview questions were used as a guideline to structure the conversations:

1. How is the cyber risk management structure in your organization arranged? (for this also: what is the organization design like?)
    a. Do you follow the three lines of defense structure?
    b. If not, what does the structure look like?
    c. Who are most relevant stakeholders in this structure?
2. Do you feel cyber risks are effectively managed?
3. Where is ownership for digital compliance / cyber risks placed in your organization?
4. What do you think are strengths in this approach of risk management in your organization?
    a. Which elements contribute to these strengths?
5. What do you perceive as weaknesses in this approach of risk management in your organization?
6. How do the first and second line work together in your organization?
    a. Is communication between people in the first and second line (or business and compliance teams) currently effective, or do you see a gap there?
7. Do you believe it would lead to more effective cyber risk management if there would be second line knowledge embedded in the first line?
    a. What would be your reasons to implement or not implement this approach?
    b. If yes, or no, do you see practical issues with implementing or with not implementing this?
8. If the organization structure around risk management would be created from scratch today, what would it look like to be most efficient in your opinion?
    a. What are factors of success here?
9. Are there other factors that you think contribute to successful cyber risk management that we did not cover?

Depending on the interviewee, the conversation would at times dive deeper into a specific question and briefly address other questions. When interviewing experts originating in consulting professions, the questions were tailored to accommodate the fact that they did not work in a specific organization. Here the questions were generalized towards findings of the participant when working in tech-oriented organizations.
In addition, question no 7, '*Do you believe it would lead to more effective cyber risk management if there would be second line knowledge embedded in the first line*?' was often received by confused looks from research participants, as they did not always understand what was meant by this. To give more clarity the following explanation was added: '*for example, by educating engineers in the first line in cybersecurity or privacy topics, or by hiring digital compliance experts directly into the first line to support with product development'*.

During the interviews notes were taken, which were used to later identify what answers were provided and by whom.

The following roles and organizations participated in the interviews. Interview 05 and 12 contained two interviewees, as specified below.

Interview number	Role	Organization
01	Engineer	Big tech company in the automotive industry
02	First Line Privacy Product Expert	Large advertisement / tech company
03	Privacy Leader	Medtech company
04	Chief Data Compliance and Privacy Officer	Medtech company
05	Managing partner Privacy	Consulting agency
05	Partner Information Security	Consulting agency
06	Compliance Solutions Specialist	Large advertisement / tech company
07	Cyber Information Security Officer	Publicly traded Medical Device company
08	Head of Operations, background in cyber	Fintech company
09	Sr Digital Compliance Specialist	Bank with a large focus on technology
10	Member Supervisory Board, former CRO	Financial institute with a focus on new technology in their operations
11	Senior Manager	Semiconductor Wafer Manufacturing
12	Chief Risk Officer	Large insurance company with a focus on new technology in their operations
12	Chief Security Officer	Large insurance company with a focus on new technology in their operations
13	AI Governance lead /coordinator	Entertainment industry, former consultant

5. What are the disadvantages of the Three Lines Model for companies with a strong emphasis on technology?

In the first chapters, the Three Lines Model is described, as well as the Three Lines of Defense Model on which the Three Lines Model was based. Overall, this model has increasingly been found in cyber risk management structures, sometimes formally, in other cases informally. This could also be observed in the discussion with participants: 10 out of 13 participants independently described a cyber risk management structure that either formally or informally implemented a first, second and third line, and recognized the division of responsibilities and tasks to be similar to the models.

The exceptions were interviewee no 1, who was not sure if they had implemented the three lines model, and interviewee no 4, and 13. These two interviewees mentioned elements in their organization that indicate that the three lines model is partially present, though at the same time they expressed that there is not always clarity about who to consider the first line.

Interviewee no 4 for example said: '*Risk management structures are organized across several domains within my organization. […] There is shared responsibility across the legal and the technical domain. There is an evolving conversation about who is the first line*.'

There are good reasons to implement the Three Lines Model, as mentioned in paragraph 4.3, but there is also critique on utilizing these models, especially in fast paced organizations with a strong emphasis on technology. Points of critique mentioned in literature included: lack in collaboration between lines, effectiveness and efficiency of the model, and issues around the pace with which new technology and laws are developed when using the three lines model.

Several similar and new points came up in the findings of the participants. They addressed the following four points: lack in quality of communication between lines, difficulties in creating accurate advice due to the fast pace of technology and new laws, limited ownership in the first line and fear of cyber risks, long turnaround time cyber risk processes.

Below we will address each of these points of critique provided by one or more of the interview respondents.

5.1 Lack in quality communication between lines

In organizations where there is a strong focus on new technology, it is difficult for the first and second line to understand each other.
This is for example mentioned by interviewee no 6: '*For tech companies the communication between the first and second line are more difficult'*.
This is also mentions by interviewee no 11, who explains that: '*there can be a disconnect between the centralized risk management function and the first line. The senior managers may understand each other, but the working forces do not. There is a lack of understanding what the other side needs to find solutions'*.

This difficulty in understanding can lead to situations where the advice of the second line does not match the reality of the first line. For example, the solutions from the second line may be too expensive or prevent the business from doing innovative work, because the second line does not understand the way the first line operates.
This is mentioned by interviewee no 11: '*The second line works across the business and aims to create wholistic policies. It is hard to explain to them what is needed by the business. Organizations work best when the incentives of each group align with the larger incentive. This is not always the case and it can lead to a slow down or stop on innovation.'* Interviewee no 06 describes that there is a '*knowledge gap when it comes to cybersecurity when the line structure is followed. For example: demanding 'best security' comes with a whole lot of work and problems for the first line, which is something most lawyers do not understand, leading to additional business risks. For cybersecurity it only works if the second line roles really understand the product well.*'

This lack in understanding may also occur because of a different perspective on how the business should function.

Interviewee no 09 sees this as well, and states: *they (the second line, red.) at times do not understand that achieving 100% compliance is practically difficult to do. The first line is more practical. The first line is well aware of the risks but also looks at more than just the cyber risks*.

If the second line is not able to understand the reality the first line is working with, the solutions they provide may miss their point – as in the end, any action can lead to a risk, and eliminating risks completely may mean stopping the business or significantly hampering the first line, as mentioned by interviewee no 11. To come up with risk mitigations that work well for the first line, both lines need to have a clear understanding of each other's situation and challenges. Here effective communication is key.
This is also emphasized by interviewee no 10: '*It is important to teach the first and second line to talk to each other. You need education and culture to explain to the lines how this works. They should not sit in each other's seat but must enter into a conversation with each other. Ownership cannot be forced, it should be clear to all that this is needed to do our jobs and to create products. If you enter into real conversations with each other this will come more to life. The second line has a responsibility to engage with the first line and manage good communication.'*

5.2 Difficulties in creating accurate advice due to fast pace of technology and new laws

The pace of new developments in the technological domain, combined with the pace of changes in the legal domain, make it difficult for companies with a strong focus on new tech to effectively use the Three Lines Model. Continuous updates of laws and regulations make it significantly harder for organizations to stay up to date on what is needed from a business perspective to comply with new laws and updated regulatory guidance for (new) technology. This is amplified by the fast pace at which new technology is developed. For second line specialists who want to provide guidance and flag possible risks it is crucial that they understand the technology used by the first line on a fundamental level, which is more difficult if this keeps changing.

Interviewee no 06 puts it like this: '*There is so much happening in new laws to follow, and at the same time products are constantly changing, and it is difficult to stay up to date with the product. It is hard to hire for this. You cannot have an army of lawyers, you need people that also really understand the technology of cybersecurity. In addition, new laws like AI act again come with questions about what it means on a product level.'*

Interviewee no 06 also explains that: '*New features are coming out in technology, new regulations are coming out and are often complex and not so harmonized. Navigating the ambiguity and pace are difficult, but need to be done*',

This is an important point, following a phenomenon that is often explained as the 'pacing problem' as explained in chapter 3.4, and as described in relation to the Three Lines Model in chapter 5.1. For organizations it means in addition to dealing with fast paced changes in technology they also need to deal with new or more ambiguous laws, case law and added guidelines from supervisory authorities aiming to regulate the changes in the technological landscape.

5.3 Limited ownership in the first line and fear of cyber risks

Another point of critique the interviewees highlighted, is the fact that the model requires strong ownership of the first line when it comes to risks that are flagged, and this kind of ownership is not always in place. When risks are flagged by the second line, the first line must undertake action to ensure the risk is mitigated to an acceptable level. The first line works at an operational level, and must ensure that products and services created or utilized by the company are not posing unacceptable risks. The interviewees pointed out that this responsibility is not always seen as a priority for the first line, and furthermore there might be a conflict of interests when the business sees the documented risk as something that may harm or impact the business.

For example, interviewee no 02 explains that a crucial point for risk management to succeed is willingness from the business: '*Willingness from the people involved, including the business. The business is so busy that they feel do not have time to work on risk that does not cost money if not mitigated now.'*

Interviewee no 03 calls out accountability as an element for successful risk management in the company's existing model '*Accountability of the Business Owners* (the first line red.)'.

Another downside of this lack of ownership and of accountability in the first line is that this can lead to situations where business owners try to prevent risks from being documented or flagged by the second line, for example by not engaging the second line functions. When risks are missed, or when no follow-up action is undertaken to mitigate the ones that are identified, the consequence is that the Three Lines Model becomes ineffective.

Interviewee no 7, states: '*Risk ownership [...] can be perceived by the business as a bad thing, and we need to make sure to explain that it is not. Risks are part of doing business. We want to ensure we have visibility on the risks that are present. We also need to have a list of risk owners, including information regarding the level at which a risk can be owned. I would prefer to have a multi-tier approach, having a VP that is risk owner, and then someone below that person who is driving the risk mitigation, a risk leader and/or a tech risk leader that can make the changes.'*

Participants no 12 also mentioned that the involvement from the business is limited, and gave an extra reason for this in explaining that the second line together with the IT function are doing a lot of the work relating to cyber risks. 12: '*The involvement of the business is relatively small because IT and the second line handle a lot of the cyber risks'*.

This specific and important point on ownership may apply to more domains than just cyber risk management and compliance with digital regulations. However, as the pace of innovation in these domains is high, and both technology and laws here develop fast, the issues around risk ownership and fear of documented risks are more prominent.

To quote interviewee no 01 when talking about situations where the first line is not always communicating with the second line: *'Risk can grow exponentially, which is something the business teams may not be aware off'*.

Interviewee no 07 provided a possible solution to address this: implementing a visible risk register with multi-tiered ownership and ensuring that risks are not viewed as mainly a bad thing

but that risk management, including the treatment actions, are instead seen as a part of doing business, and a part of the general business processes.

5.4 Long turnaround time cyber risk process

Another point of critique is the time it takes for second line reviews to take place. Interviewee no 09 states it this follows: '*It can be cumbersome for the organization to go through all three lines. All lines have a lot of work, the weakness is that people in the business try to circumvent the process/second line because it takes too much time. We should take shorter to support the business.*
Sometimes it can feel like I am an adversarial role. It is about making the company safer. This may be hampering innovation a bit, as things take longer.'
And interviewee no 10 notes that for cyber risks '*the three lines do not seem to work because it takes too long when it comes to policies, which cannot be altered fast when an attack occurs, which is when action is needed. The second line creates cyber risk policies and needs to ensure that these are suitable despite rapid changes*'.

Taking all four points of critique into consideration, it becomes clear that there are significant disadvantages to the model, which can lessen the effectiveness of the model's operation, or even worse: to an increase in risks. In the following chapter we'll take a closer look at a new approach, to see whether this may eliminate the disadvantages of the existing model and at which price.

6. What are the advantages and disadvantages of consolidating second line knowledge with the first line?

6.1 Second line knowledge in the first line: the Three Lines Bridge Model

As shown by the interviewees, the organizations aim to deal with the above mentioned critique in different ways. One approach which has recently been gaining popularity in companies with a strong focus on technology is to establish or re-enforce second line knowledge -for example knowledge about relevant laws and regulations, company risk policies, and risk appetite- in the first line. There are different ways to do so, as described by the interviewees. Here a modification on the Three Lines Model becomes visible in organizations, where a knowledge bridge is build between the second line and the first line. In this thesis, when referencing this modified version of the Model, it will be named the *Three Lines Bridge Model*.

6.1.1 First line employees participate and anticipate

One way we see that knowledge is brought into the first line, is by requesting the first line to initially assess possible risks themselves, before engaging the second line. This is the case in the organization of interviewee no 08. '*Risk is structured following the Three Lines Model. [...] The first line needs to understand compliance, and is making a first assessment before talking to the second line. For big projects (e.g., DORA implementation) there is also a project manager*'.

This means that the first line needs to be able to perform these assessments and understand second line requirements.

Another way to bring second line knowledge into the first line, as illustrated by several interviewees, is for companies to facilitate training and education on second line knowledge for the first line. Some organizations propose to have second line 'trained champions' in their first line teams, such as security and privacy champions. Interviewee no 04 mentions on this: *'Another approach, is to have a robust ambassador program within the organization. This involves people whose day job is the tech job, but they have been trained to better understand specific simple digital compliance questions.'*

6.1.2 Implementing a separate Bridge 1.5 role

To bring second line knowledge into the first line, some interviewees have come up with a different approach. They describe the first line hiring employees that are dedicated solely to activities related to second line requirements, thus functioning as a bridge for the first and second line. These roles, or as we will call it in thesis, the *Bridge 1.5 roles*, are for instance present in the organizations of interviewees no 02, 03, 06, 07, 09, 12 and 13. These bridge 1.5 employees have strong knowledge of the first line and their products and processes, in addition to understanding requirements from a risk management and compliance perspective.
Interviewee no 2, briefly quoted above, explains: '*We have smart people in the first line that know the product technically inside and out. These people used to be working as engineers and are home grown into privacy experts*'.
Interviewee no 09 provides another example: '*I am part of the first[t] line as compliance. I verify the work of colleagues in CISO teams, I function as a 1.5 role.'*
Interviewee 13: '*We also have a 1.5 role that is more involved in the first line'*.

These ways of including some form of second line knowledge into the fist line comes with benefits, but there are also downsides to this. In the next paragraphs both sides will be discussed.

6.2 Benefits of the Three Lines Bridge Model, bringing second line knowledge into the first line

Benefits for the interviewees of adding second line knowledge in the first line as described in the adjusted application of the Three Lines Model, here called the *Three Lines Bridge Model*, can be clustered into the following:

- Informed conversations leading to more accurate cyber risks
- More open attitudes towards flagged cyber risks and mitigations by the first line
- Improving turnaround time of cyber risk reviews
- Feedback loop for lawmakers

6.2.1 Informed conversations & more accurate cyber risks

Knowledge of second line requirements present in the first line makes it easier for well informed conversations to take place between first and second line parties, and risks and requirements become more accurate and specific in the context where they occur.
The earlier quote by interviewee no 02 makes clear that in her company, there are '*smart people in the first line that know the product technically inside and out. These people used to be working as engineers and are home grown into privacy experts'.* Meaning there are people with second line knowledge working in the first line. The result is seen as very positive, as interviewee no 02 explains that it '*makes them (the 1.5 people, red.) better at supporting privacy compliance and also means that they speak the language of the engineers'*. And so, the reason why this set-up is perceived as positive, is because 'they speak the language of the engineers', thus facilitating better communication. This communication is crucial in order to establish accurate cyber risks. The second line employees may have an understanding of what an internal risk policy may state, what a law requires, or how a control should be implemented, but to understand whether or not the technology complies with this requires a complex trade-off, for which they are often dependent on information from the first line. If people in the first line fully understand what is needed from the second line, they can support the issue by providing relevant information, enabling the second line to make accurate risk assessments.

This is supported by statements of some of the interviewees.
Interviewees 05 explain when asked about including second line knowledge in the first line that the second line *'may understand the law but what it actually means on a product level and on a tech level is often very difficult to translate. The 1.5 person really needs to understand the product, and why certain decisions relating to the product were made'*.
In addition, interviewee no 07 elaborates on the importance of the right context being present for the second line, when asked about the application of second line knowledge in the first line: '*I think this would be a good way to accelerate the risk assessing. If context is missing in the second and third line, it is difficult to manage risks. In our organization we are implementing second line knowledge in the first line for security product and for privacy reasons. Conflating these lines contributes to better risk management.*

Interviewee no 03 states this as well: '*It is challenging for engineers to figure out (how to deal with red.) compliance requirements by themselves, having compliance knowledge in this line is therefore helpful.*' Another quote of this same interviewee emphasizes the importance of the close collaboration between the first and second line: '*The best design ideas come from engineers, so we need to talk to them. Make them part of the solution.*'

To conclude, for organizations with a strong focus on technology we see that when including second line knowledge in the first line, both communication and collaboration between the lines improve, leading to better context for the second line to flag accurate and specific risks. According to the participants this enhances effective cyber risk management.

6.2.2 More open attitudes towards flagged cyber risks and mitigations by the first line

Another benefit of having second line knowledge in the first line is that this leads to a more welcoming approach from the first line to flagged cyber risks, and with that, to more effective mitigation of these cyber risks. If employees in the first line have a better understanding of the

requirements and risks as perceived by the second line, and if the requirements set by the second line are more tailored and made relevant to the technology and the reality the first line encounters, there is a bigger chance the first line will want to act upon these. Interviewees express similar ideas and observations, adding that the first line in that case is better equipped to mitigate initial risks themselves.

Interviewee no 03: '*Another strength of our approach is that risks and mitigations are better received. We cannot expect the business to understand all risks, but they become more aware of risks and can mitigate obvious privacy risks themselves. For example when it comes to a vendor not having or wanting to sign a DPA (Data Protection Agreement red.), the business owner (in the first line, red.) can already flag this.*'

Interviewee no 10 adds to this perspective that the first line is more receptive to ownership following good communication. As quoted before in section 5.2.1: *'Ownership cannot be forced, it should be clear to all that this is needed to do our jobs and create products. If you enter into real conversations with each other this will come more to life.' The second line has a responsibility to engage with the first line and manage good communication.'*

Interviewee no 08, working in an environment where the first line does an initial risk assessment before talking to the second line, explains that when following this model '*Ownership is much broader, and there is understanding of what needs to be done in the first line because of obligations'*.

Following this information from the interviewees, it becomes clear that when the first line is equipped with sufficient knowledge, be it via additional communication and training, or by requiring the business to assess risks before discussing new products with the second line, the ownership for these risks will be strengthened, and acceptance of the importance of addressing cyber risks increases.

6.2.3 Improving turnaround time of cyber risk reviews

In addition to the above mentioned benefits, interviewees indicate that by incorporating knowledge from the second line into the first line, risk review delivery times decrease.

This point is touched upon earlier in the quote from interviewee no 03. '*We cannot expect the business to understand all risks, but they become more aware of risks and can mitigate obvious privacy risks themselves. For example when it comes to a vendor not having or wanting to sign a DPA the business owner can already flag this.*' Here we find a clear example of a risk that can be flagged and immediately addressed or prevented by the first line. If the first line recognizes that a possible future vendor does not want to sign a DPA, they can decide not to engage with them, and instead choose a party that does want to sign the right agreements. In this case, additional steps where the second line needs to flag this as a risk, and the follow-on steps of engaging in a formal risk procedure, leading to risk conversations taking place, mitigating measures needing to be documented, reviewed and executed, further monitoring of the risks, etc. will not be necessary. A significant number of additional steps can thus be removed from the process.

In addition the interviewee is of the opinion that one of the goals of the first line is to limit the turnaround time for reviews and to support the first line as much as possible: '*When it comes to developing and engineering teams more in depth privacy support is needed, if you are doing this old school with one centralized compliance hub it soon becomes more difficult and time consuming.' 'The challenge and our goal is to translate customer expectations and privacy regulations to privacy requirements and to Jira tickets. This empowers the first line business to do their own work, and enables the privacy team in the first line to review this work and support with more complex questions.'*

Enabling the business to identify possible risks and mitigate these before the second line reviews is also mentioned by interviewee no 09 when asked for his opinion on the idea of placing second line knowledge in the first line: '*Yes, that is a good idea, once you are aware of something, you can do something about it. This enables the business to make informed decisions about cyber risk. My colleagues are SMEs (Subject Matter Experts, red.) in their own areas, and awareness helps them. Awareness is more relevant than knowledge itself. You need to have awareness. Knowledge is needed for other topics, people are overloaded with knowledge.'*

6.2.4 Including feedback loop for lawmakers

A point that has less to do with the direct results of an organization, and instead is seen as an overall benefit, is the fact that the Three Lines Bridge Model facilitates a better feedback loop to law makers by bringing in knowledge into the first line. 06: '*Our business is able to provide input on how to implement new laws and regulation but also on how to respond to draft laws and consultations. This is the strength of the 1.5 line employee'*. And *'There is also a good feedback loop from the business on how to implement laws and regulations and legal drafts etc., this enables us to respond to proposed regulations when they are in the consultation phase.'* It would be interesting to further research how this impacts legislating decisions and if this leads to a better fit between new technologies and laws regulating these.

6.3 Disadvantages of bringing second line knowledge into the first line

Next to the benefits of bringing second line knowledge in the first line, there are also downsides to this. Especially when the so-called Bridge 1.5 role is mentioned, there are concerns from the interviewees. These include:

- Relevance of information brought into the first line, and high investments
- Losing responsibility and missing cyber risks

In this section we will look at these issues, as provided by the various interviewees.

6.3.1 Relevance of information brought into the first line and high investment

Several of the interviewees did not think it would be a good idea to include second line knowledge into the first line, or voiced concerns.
Interviewee no 1 mentions the following: '*At my organization it would not be practical, there may be situations where this could lead to communication being shared that is not applicable to the business. A risk of this approach is that the engineers are spending time on information*

that is not relevant for them. It could work if the right information is shared, and for big organizations it means that the right people or teams (compliance and business wise) need to find each other.' Adding second line knowledge to the first line can be an extra burden, imposing additional training and education which is not relevant for the work of the first line employee. Only if specific, tailored information is provided the approach could work.

Interviewee no 04 highlights that Bridge1.5 roles can be implemented, but require investments from the business and additional training to support culture for it to be a success. '*It is not clear if adding second line knowledge in the first line is really working or if it creates roles with split personality where privacy/security employees work with the business and then review them. You could train engineers to be good privacy professionals. Another way of addition second line knowledge in the first line is to let compliance resources live in business teams. These examples are possible however they require significant investment*' and '*Elements to make this a success include organizational commitment that needs to be demonstrated and shown by additional resources, and additional training to support culture.*'

Interviewee no 06 provides additional concerns: '*The number of skilled people is not sufficient. If teams depend on the 1.5 people we need enough of them*'

Interviewee no 11 sees no added value of bringing in second line knowledge into the first line, for yet another reason: his experience in the organizations that he has worked for leads him to conclude that it would not be practical for these specific organization types, since compliance is too small a part of the product: '*In companies I worked for this would not work. This could work in companies where compliance is a larger part of the product but in my case this makes no sense.*'

These examples from the interviewees show that there are some significant downsides to implementing second line knowledge into the first line. The first example illustrates the importance of only sharing relevant and pointed information. Most people working in businesses have more than once experienced training and awareness trajectories that seemed irrelevant to their work, which is time consuming and burdensome. Furthermore, including a Bridge 1.5 role in the first line is costly, as there is a scarcity of this knowledge, and for a certain type of organizations this is not needed, when compliance is not a big part of the product.

6.3.2 Losing responsibility and missing cyber risks

Another downside to including second line knowledge into the first line is that this may lead to missed risks due to the first line being incentivized to downplay risks, or risks are not recognized as such.

Interviewee no 08: *'People may be incentivized to interpret risks in a manner that is more convenient, or to miss the significance of a risk'*. Interviewee no 03 adds to this perspective by describing situations where a lack of business involvement -by purpose or by accident- could be observed: '*A weakness can be a lack of business involvement. If you leverage risk identification to the business it can lead to incorrect decision making by the business, purposefully or by accident. It is a balancing act to ensure the right decisions are made by the business. For example: a business owner should not be reviewing (content of, red.) DPAs'*

Interviewee no 04 has concerns on how to retain a balance when determining which decisions can be made by the first line: *It can be a challenge to interpret the risk appetite to concrete situations, and someone needs to ensure that on an individual basis the risk appetite is safeguarded*.

This is an important concern, as missed risks impede effective risk management.
Interviewee no 03 provides a solution: '*To solve this you need a strong third line audit role*.'
It would be interesting for future research to investigate the effect of the third line.

Another concern relates to loss of ownership and responsibility for risks once a Bridge 1.5 line is in place and takes over (part of the) the risk related work over from the first line. Interviewee no 13:'*I think the business should be responsible, which you miss out if you have the 1.5 role*'.
Interviewee no 10 refers to this as well: '*Requirements must be laid down in functional terms, and good requirements must be established. Let the first line explain how they will do that. 1.5 roles reduce ownership in the first line*'.
Interviewee no 08 works in an organization where the first line does a lot of risk related work. In this case, the second line is required to do an initial risk assessment before talking to the second line about new products and services and sees something similar in her organization. Although people may miss risks, there is a lot more ownership due the chosen approach of less support for the first line, thus forcing them to do more risk work: *'Ownership is much broader, and there is understanding of what needs to be done in the first line because of obligations'*.

7. What are the key factors of success in organizations where the Three Lines Model is implemented?

In the previous chapters research has been conducted on the advantages and disadvantages of adding second line knowledge into the first line.

With regard to the advantages, the question arises whether we can define specific factors or circumstances that are essential for the success of the Three Lines Model, or a hybrid version of the Three Lines Model, the Three Lines Bridge Model as described earlier. For this, the interviewees were asked which elements were important when looking at the strengths of their organizations' approach to cyber risk management. Especially in cases where the respondent indicated to have implemented some adjusted form of the Three Lines Model, it is interesting to gain insights into how to make the model work effectively.

A significant amount of input was provided by the various interviewees. The input is related to company culture and structure and it can be clustered into six sections:

- Support from top management
- Education
- Contact and collaboration between teams
- Organizational structures
- Ownership

- More transparency by digitizing

In the below paragraphs these sections are further discussed.

7.1 Support of top management

Most respondents agreed on the fact that support from the top, both in communication and acting is crucial to ensure that cyber risk management and the Three Lines Model can become a success.

Interviewee no 05*: 'The tone from the top is very important for successful cyber risk management. If the CEO / management team is not supporting cyber risk management, all programs around this will struggle. In addition, it is key to build a strong culture around digital risks and compliance within the organization itself.'*
Interviewee no 03 also named: *'business and leadership endorsement'* as an element for success.
Interviewees no 12 (part of top management) says something similar: '*The top of the business is very aware of the importance of cybersecurity, and we pass this on to the business, we give the topic attention on the intranet, and make e-learning mandatory. We also have fun campaigns.'*
Respondent no 07 adds to this perspective that in addition to the right tone at the top, companies also need to empower the people leading or building out cyber risk management teams. These leaders in turn must engage the right people and communicate with these key stakeholders, including the board: '*First, you need to have an empowered leader that can communicate well and engage the right people (VP, board, etc.), this person will create the framework, standard and rules of the road for the team and governance structure. This person will be empowered to build the program'*. Respondent no 13 confirms this: *'Tone from the top is important, engagement from leadership is crucial.'*

7.2 Education

In addition to the tone at the top, investing in education is also seen as an important factor as well. Interviewee 13 sees that employees want to be supported by AI and look for training on how they can best utilize this. He proposes to integrate compliance training in the training about how to use AI tools. *'Invest in employees and training, a lot of employees want to be trained on AI, and how they can be supported by it. We can include compliance into these conversations.* Education is also named by other interviewees. For example, interviewee 06 describes that in addition to 1.5 lines supporting the first line, employees must be educated, as the amount of work for this line will otherwise be too much: '*Elements that contribute to success are a strong culture of security, and education to employees, because the 1.5 line cannot manage all the risks as the scale is so big.'*
Interviewee no 07 adds that the education should not just be in place, but also be well documented*: 'What is also important, is having formal documented training.'*

Interviewee 03 specifies upskilling as a factor of success: '*Upskilling privacy employees and legal teams, as digital compliance is becoming more technical, compliance functions need to understand the technical environment. Otherwise we end up with paper compliance.'*

7.3 Contact and collaboration between teams

In addition to company culture, contact between employees and close collaboration between teams and lines is another important topic mentioned as a crucial factor for success. This can be dealt with in simple and practical ways, such as catering to time zones as mentioned by interviewee no 2: '*One change I would make is to change it to cater more for time zones'*.
Or it can be addressed with a relationship oriented attitude, for example by ensuring that there is trust between employees. Interviewee no 07 mentions this: '*Trust is crucial. This supports speed in risk management. Having conversations builds trust, and trust is built over time'*.
Interviewee no 04 emphasizes the importance of offline connections*: 'Face to face contact between colleagues is important, especially in remote working. If you skip this part, you miss the opportunity have informal conversations and norming'*. The interviewee also explains that this can be a challenge for second line functions as they are not as widespread as the business they support. This respondent provides a possible solution by making sure the second line is invited at the right moment instead of being constantly continuously present: *'This is difficult for compliance teams, as they cannot join in all business team meetings. We need organization-wide dedication to ensure the compliance functions are invited at the relevant moments to be most effective.'*
Interviewee no 08, working in an environment where the first line is asked to make initial assessments for digital compliance and cyber risks, also underlines the importance of an interpersonal approach: '*Having an interpersonal approach and understanding that we all want to get to the same point. Minimize hostility between teams and facilitate early engagement when it comes to thinking about cyber risks.'* Interviewee no 07 adds that for Bridge 1.5 roles, the first line needs to feel comfortable with this new role and to be open to accept the new person: '*To succeed, we need to make sure that business teams embrace the new knowledge/role in their teams. If they are worried about the new person being there to audit/monitor, then it becomes really difficult to be successful.*
He continues with a solution in the form of expectation management: '*This can be avoided by setting the proper expectations',* and by ensuring the person in the Bridge 1.5 role is sufficiently enabled to live up to the set expectations: *'You also need to ensure that the 1.5 person is able to execute on the requirements and support the business. When doing this we need to be clear about the timelines for privacy/security work, while at the same time empowering the 1.5 person to deliver on the assignment. This assignment can include activities to support the cyber risk management.'*
In words of interviewee no 02 regarding elements contributing to success: *'(it is a, red.) unique combo of being a bridge, understanding tech details and talk about it in a way that is not too legal and practical. Translating between the teams and making compliance digestible.'*

Interviewee no 07: '*Risk management is an evolving process. Our strength is collaboration, this can not only be done by our own team. We have ERM that we work with, but our approach also enables us to ensure we have the business perspective, and that we can align our risk appetite. This enables us to have a full picture of risks and their impact on our organization.*
The importance of an interdisciplinary approach to risk management is further elaborated on by interviewee 07: *'You also need to have conversations with the enterprise architecture team, having an architect review board with an interdisciplinary group of different tech folks*

understanding risk. Then having analysts around good tools, the analysts also need to have good conversations with the business, understanding them.'

7.4 Organizational structures

Another relevant factor that was named is the structure of the organization, and how the handling of cyber risks is organized within the entire organization.

For example, interviewee no 02 states: '*We do not quantify everything as a companywide risk. We follow the policies but also have an internal team compass per team. This may change when people change. The silo or pillar structure makes this worse.'* This is an example of how a company structure (where there are several silos in place) can harm successful cyber risk management, especially when the siloed approach from the first and second line is strengthened by having Bridge 1.5 roles in place that work with one specific part of the business and no overarching or centralized risk management teams.
Interviewees no 05 explain that they see that cybersecurity is, more often than not, split into an operational part of information security (in the first line) and a governance, risk and compliance part (the second line). *'Increasingly, cybersecurity risk is split into governance risk and compliance (often falling under the CISO), and an operational part of infosec, placed in an operational team. This team has operational, technological and architecture related responsibilities.'*

For privacy risk management they see a similar split, particularly in more mature organizations. '*For more mature organizations the privacy risks are owned by separate resources or functions, in a hybrid model. Sometimes part of these functions (legal related) report to the General Counsel, while an operational privacy team is part of the product team.*
As it is difficult to have various privacy teams to support different functions you do not see this often, except for a few big tech companies. Instead it is more common to have a more centralized privacy team supporting various business functions'.

Interviewees no 5 add to this that for privacy specifically a hybrid model is preferred for mature organizations, but for small companies a more centralized approach works better, as this can be scaled up more easily. '*It depends a bit on where the company is in their journey. If it concerns a small company, a much different and more centralized organization is needed. If the organization is more mature, a hybrid model where certain things are performed centrally but more operational tasks are performed and monitored more decentralized is also a good option. A hybrid model is preferrable over fully decentralized to ensure that monitoring is easier and so that organizations can facilitate knowledge sharing, and for performing tasks that apply to all parts of the organization*.'

Interviewees no 05 elaborate on the consequences of centralized and decentralized organization of cybersecurity and privacy: '*Another important distinction regards centralized or decentralized organizations around cybersecurity. If there is a strong push to strengthen the cyber security function in organizations, for example after an incident or audit finding, that drives setting up a centralized organization, as this is easier to scale-up. More mature organizations will want to distribute cyber security to have a stronger push towards more distributed ownership in the business. This is more likely to be found in mature organizations'.*

Interviewee no 06 would organize the cyber risk management structure in a similar way when asked: '(a, red.) *more decentralized approach, larger decentralized organization compared to centralized organization'*.

For well-functioning AI compliance structures there is still unclarity on where to place cyber risk management in an organization. Interviewees no 05 explain: *'For AI risk management we are still developing structures in organizations as this is relatively new.'*

Another point of attention is the fact that reorganizations can have a negative effect. Interviewee no 06 states that '*Reorganizations are also making it more difficult, a lot of tech companies are reorganizing to try and get the right structure, but this has a lagging effect'*.

Interviewee no 11, working in the business as part of the first line, has an opposing perspective when it comes to structuring the organization following a hybrid model. On being asked about strengths of their organizational structure the response is the following: '*The first line does not have to think about risks and compliance too much. It is managed by a unified function. This means that not each group needs to hire their own lawyers and second line employees. Centralize all the enterprise functions.'* This interviewee works as a participant in the business, and thus shares his perspective as someone not working in a compliance function, and in this statement makes clear how the business is impacted negatively when there is a decentralized approach, considering the consequence that the company has to hire multiple lawyers. It must be noted that this interviewee is one of the few that works in an organization where there is no first line knowledge present in the second line, and where this is deemed unpractical by the interviewee.

Other elements contributing to success when including second line knowledge in the first line, relate to organization structure include maturity, as already touched upon before, and how the new roles such as the Bridge 1.5 role fit in the company structure. Interviewee no 03 mentions these elements specifically: '*Maturity of the organization, and new roles tying into this.'*

7.5 Ownership

Lastly the interviewees show that for the Tree Lines Model in Cybersecurity to work, ownership and transparency is needed, supported by transparent tooling or digitization where possible. Ownership here must not be limited to acknowledgement of responsibility for a team, a task or a part of the work. It goes beyond that, and also means proactivity and willingness to commit to get the best possible results. When managing cyber risks, ownership is key. Appropriate incentives for the first line and business owners can help establish this ownership. Interviewee no 02, working in a Bridge 1.5 role, named willingness of the business when it comes to involvement into cyber risk management as a weakness when using the Three Lines Model. Interviewees no 12 emphasizes that having ownership in the first line is a key factor for success and explains that they have central oversight meetings where the first and second line meet, thus ensuring visibility. In addition, existing processes are evaluated on their effectiveness. This transparency supports ownership, as mentioned by interviewees no 12: '*Ownership in the first line is an important factor. We have an overview meeting where*

everything is centrally discussed by the risk teams, so there is an overview. We then evaluate whether the processes are working and discuss what we see and what we don't see.' Interviewee no 06 states that she thinks it is important to highlight risk ownership and enable risk owners in the first line, so that they can mitigate or work on the risks based on what is needed. She also thinks an important factor for success is to have more transparency in how risks are assigned and proposes to have this documented in a specific type of matrix (a RACI Matrix). No 06: '*Then you need to understand who owns risks and ensure they are supported sufficiently based on the size of the risk they are carrying. I would also like to see more rigor in risk management, to include a RACI per risk, identifying where it sits'*.

7.6 More transparency by digitizing

Transparency coming from technical tools and digitization came up as another important element for risk management be successful. This enables effective limitation of risks even more. Interviewee no 10 highlights the importance of automating risk management, by having good controls supported by sensors which measure if controls work. The interviewee explains that where possible, this process must be supported by deploying AI to interpret the results due to the large number of notifications that need to be reviewed. This will provide transparency for the organization: *Controls ensure that your systems remain secure, checking if everything is in order. Additionally, it is important to implement many (self-learning) sensors that measure whether the controls are working. You then report on which sensors provide resilience. This is all part of the first line.' And: 'It is also important to digitize your control framework and make it part of daily routines. This must be managed in the first line. By letting the sensors and controls do the work, you have less work and the system creates exception reports. Deviations can be used to report to the second line and the third line'*.

By following these recommendations, additional transparency is provided on risks and how to manage these. The first line works on ensuring and showing initial risks and communicates to the second line about them. The automated reports support ownership in the organization. This is also in the interest of the business, as mentioned by interviewee no 10. He explains that the whole point of risk management is to add value for the company with limited risks. For this: *'digitization is crucial. The last thing you want is for a change in your processes or product to create risks. This aligns with the desire from risk management teams'*.

Interviewee 07 also highlights the need for tooling: '*There should also be a good tool for risk management, documenting risks and historical decisions'*. The interviewee also sees the need for analytics and reporting, something that will enhance transparency: '*Lastly you need a governance focused on analytics and reporting, defining key risk indicators, encompassing being proactive and limiting risk'*. He mentions that tooling should not be done if the organization is not mature enough: '*Do not automate too early if you are not ready yet'*. *Lastly he explains that using security frameworks can be beneficial however they should be tailored to the organization that they are used in. 'Frameworks help structure how to potentially do something, but it should not lead to a one size fits all. Security is not only science but also an art'*.

8. Analysis, research limitations and proposed further research

The interviews conducted for this research have provided significant information about- and insights into the Three Lines Model in tech-oriented companies. This did not only lead to answers to the sub questions and research question, but it also led to finding additional information that could not be investigated due to the scope of this thesis but is worth exploring further in the future. This is elaborated on in this chapter. Next to that, the limitations in the present research of this thesis have been listed in a separate paragraph.

The interviewees have given input on factors or elements that can contribute to a successful implementation of the Three Lines Model, and on successfully implementing second line knowledge into the first line. The down sides of the Three Lines Model when applied to cyber risk management became visible as well, and information has been obtained for a possible solution to these, centering around the idea that second line knowledge is brought into the first line.

With this input, the three sub questions supporting the research question can be answered.

a) What are the disadvantages of the traditional Three Lines approach for large companies with a focus on technology?
b) What are the advantages and disadvantages of consolidating the second line knowledge in the first line?
c) What are the key factors of success when implementing the Three Lines Model in large organizations with a strong focus on technology?

Below these questions will be addressed. Based on the answers to the sub questions, in chapter 8.4 the main research question of this thesis will be answered:

Can an approach where the traditional second line knowledge is brought into the first line lead to more effective management of cyber risks, and if yes, what elements are crucial for this approach to be successful?

Furthermore, information from the interviews, as documented in the previous chapters will be analyzed, and conclusions and recommendations will be provided.

8.1 What are the disadvantages of the traditional Three Lines approach for large companies with a focus on technology?

The first sub question is answered by the interviewees who shared insights in challenges they encounter in their company's approach, showing why the Three Lines Model is not always well suited for organizations with a strong focus on technology. They came up with four major challenges:

- Lack in quality of communication between lines
- Difficulties creating accurate advice due to fast pace of technology and new laws
- Limited ownership in the first line and fear of cyber risks
- Long turnaround time for the cyber risk processes

Some of these points were to be expected, as they align with the critique we find in literature. In chapter 3 we described the lack of collaboration between the first and second line, and the difficulties around fast paced changes in technology and law. These two points are reflected in the responses from the interviewees. With regards to collaboration for example, interviewees mention the lack of good communication between the first and second line as a problem. They explain that it is hard to work together when the second line does not understand what the first line needs. The critique in literature relating to the fast changing laws and technology is also reflected in the interviews. One interviewee noted for example that it is a challenge to stay up to date on latest laws and technologies when they are constantly subject to change.

Beyond these points of critique on the Three Lines Model which were also found in literature, respondents identified two additional challenges: limited ownership in the first line and the long turnaround time of the cyber risk processes. Limited ownership relates to the fact that the first line does not take sufficient action to mitigate the risks that are assigned to them. As an underlying problem for this, the fear of being assigned risks for their processes is mentioned. This issue is an important one for cyber risk management, as lack of ownership can mean that risks are not mitigated in a timely manner. As one of the interviewees mentions, it is not possible to mitigate risks if the business does not have the time to do so. The various responses give the impression that business incentives to own and mitigate risks is at times missing in the version of the Three Lines Model they work with. It would be interesting to see how and if this problem appears in other types of organizations, that have less focus on technology. The long turnaround time of the processes in the three lines model were also mentioned by interviewees. This may lead to the first line circumventing the second line, or lead to issues when policies from the second line are not well suited to facilitate the changes in reality, or when action is needed for example during a cyber attack.

These two challenges -limited ownership and tong turnaround time- newly discovered by the interviewees, warrant further investigation. Do they occur in other sectors as well, or are they unique to technology focused industries? Is this also a an issue in other risk domains outside of cyber risk? And if so, what solutions have been implemented or must be proposed to address them? Exploring these questions could give us valuable insights for redefining the Three Lines Model across various contexts.

8.2 A possible solution: the Three Lines Bridge Model ands its strong and weak points.

When being asked about including second line knowledge into the first line, various interviewees discussed points in favor of this idea, and even explained how their organization structure around cyber risk already facilitated this. In addition to the upsides, some interviewees also raised concerns about this approach.
In order to make a clear distinction between the traditional Three Lines Model and the modified version of the model where second line knowledge was included in the first line, as seen during the interviews, this thesis introduced the name *Three Lines Bridge Model*. In this variation of the model knowledge of both the first and second line come together in the first line.

In the next section the benefits and concerns with regard to consolidating the second line knowledge in the first line, the so-called *Three Lines Bridge Model*, are addressed and compared to the downsides of the traditional Three Lines Model in order to see if this can solve some of the downsides of the traditional model. With regard to this adjusted Three Lines Model some disadvantages are also mentioned, and are addressed below as well.

8.2.1 The benefits of an adjusted Three Lines Model

There are several benefits for organizations named by interviewees with regards to second line knowledge being brought into the first line. These benefits can be clustered into the following categories:

- Informed conversations & more accurate cyber risks
- More open attitude towards flagged cyber risks and mitigations by the first line
- Improving turnaround time of cyber risk reviews
- Including a feedback loop for lawmakers

The first one *'informed conversations & more accurate cyber risks'* relates to the communication between the first and second line, and the better flagging of risks. As explained by several respondents, the first and second line often do not understand each other, the business often does not provide input that is needed by the second line, and at the same time the second line often misses important context about a product or service as they do not understand how the associated technology works. This was mentioned as one of the down sides of implementing the traditional Three Lines Model. By bringing second line knowledge into the first line, this downside is significantly reduced. Interviewees explain the benefits of adding a 1.5 role as a bridge between the first and second line. The enhanced conversations between the lines in turn lead to more accurate risks being flagged.

The second point that was mentioned *'more open attitude towards flagged cyber risks and mitigations by the first line'* addresses another element.
When the fist line becomes more aware of why a risk is flagged, especially when this is communicated by someone in their own line, they are more likely to accept the risk and do something to mitigate it. Part of this enhanced risk ownership could lie in the fact that the risk will be more accurate and tailored, as mentioned in the previous point, and partially in the fact that when the first line understands the requirements from the second line, these can be addressed proactively. The example of this being given by an interviewee is about a possible new vendor who indicates during contract discussions that they do not want to sign a specific privacy agreement. If the business understands upfront that this agreement is a requirement from the second line, they can filter out vendors that do not comply with this. In these types of situations, the first line proves to be a strong driver for compliance, and as such, shows a kind of ownership that most interviewees indicated was missing in the standard Three Lines model implementation.

The third benefit mentioned, *'improving turnaround time of cyber risk reviews',* relates to the improved turnaround time of the assessment of cyber risks. This point builds on the example illustrating first line employees performing second line tasks as a result of their awareness of the requirements needed. If as in the example given, only vendors are selected that will sign

required contracts relating to personal data, the time that the second line needs to review the vendor will be shorter and chances of the vendor being dismissed at a late stage and the business therefore having to look for a new one late in the process becomes lower. In addition, interviewees indicate that when there are Bridge 1.5 roles present, these people can take over work from the other first line employees, which will also speed up the process. This shows that by including second line knowledge into the first line, either by including a Bridge 1.5 role or by ensuring the business is trained on second line requirements, the downside of timely risk reviews can be addressed.

A fourth benefit '*Including a feedback loop for law makers*' impacts organizations less directly, but instead will lead to improvements in the entire ecosystem in which organizations operate. If lawmakers receive better feedback from the business, they can create better suited laws, leading to less difficulties from organizations and preventing situations where the law does not fit to the technological reality.

It would be interesting to conduct a more in-depth study on the second and third benefits of including second line knowledge into the first line. For example by comparing the numbers of mitigated risks in two types of organizations: on one hand the organizations where they have a Bridge 1.5 line or additional training and education for first line employees, and on the other hand those organizations where they do not have this.
Another interesting metric to study would be the timelines of risk mitigations, and whether this actually differs in organizations with second line knowledge in the first line compared to organizations that do not have this.

8.2.2 The concerns around an adjusted Three Lines Model

Downsides of- and concerns about the inclusion of second line knowledge into the first line were named as well. These are as follows:

- Relevance of information brought into the first line, and high investments
- Losing responsibility and missing cyber risks

'*The relevance of information brought in the first line, and high investments'* is one of the concerns. One interviewee explained that second line knowledge in the first line should be relevant, otherwise it adds to information and time spent without adding value for the employees in the first line. When providing training to first line employees, this should be given serious attention. It would also be interesting to see if including a Bridge 1.5 role could play a role in ensuring that cyber risk and compliance information provided to the first line is tailored sufficiently to the specific first line employees that receive the information.

More concerns raised address the high costs of including trained Bridge 1.5 line employees in the first line. Depending on how you address second line knowledge in the first line, it can be expensive both by hiring and by educating these employees. Hiring a large group of Bridge 1.5 line employees is not only difficult due to scarcity, but also expensive, because of their specific knowledge. A cheaper solution could be to educate the first line on a less complete expert level, thus making them a better partner for the second line. Here the previous comment about

relevance must still be taken into account and it must be ensured that precious time of employees is not wasted, as employee time directly translates to salary costs and productivity.

A second point relates to '*missing risks due to assessments by the business'*. Missing relevant risks either on purpose or by accident is a problem that can be approached from two different angles. It may be addressed by a strong third line that verifies the effectiveness of risks and controls. According to one of the interviewees automating controls and reviewing outcomes can be of support here, as this will give a clear baseline for the first and second line to build their conversations on. In this thesis the role of the third line has not been discussed in depth. It would be a valuable contribution to the findings in this paper to continue research into how a third line can contribute to some of the points raised, such as the possibility of missing risks when the first line is more knowledgeable on second line requirements or has the capability to flag initial risks in a first assessment.
Another point of view on this has to do with ownership in the first line for risks that may occur. If a Bridge 1.5 role is included, this may lead to losing responsibility and ownership for risks in the first line. This idea is supported by literature, explaining that if we rely on rules to tell us what is right and wrong, people lose interest in determining what is right and wrong themselves, and instead do what is allowed.[87] This can lead to an organizational culture in which people just do the work they are appraised for. In this light, moral skills can be seen as muscles: when not trained regularly they will disappear.[88] This can be problematic particularly in an environment where there is no clarity on what is allowed yet, which is often the case for new technology. It is precisely this kind of environment in which it must be ensured that new technology is not imposing risks on people and society, and so the dependency on the moral skillset of the developers in the first line is much higher than in the more traditional businesses.

8.3 Elements to make the Three Lines Model a success for cyber risk management in organizations with a strong focus on technology.

In order to make cyber risk management in organizations that implemented some form of the Three Lines Model a success, several points are indicated by the interviewees. These can be grouped into six clusters:

- Support of top management
- Education
- Contact and collaboration between teams
- Organization structures
- Ownership
- More transparency by digitizing

[87] Schwartz, B. (1994). On morals and markets. *Criminal Justice Ethics, 13*(2), 61. Retrieved from https://login.ezproxy.leidenuniv.nl/login??url=https://www.proquest.com/scholarly-journals/on-morals-markets/docview/1297908397/se-2

[88] Moerel, L. (2020). Why this risk management best practice is not fit for digital innovation. *IAPP*. https://iapp.org/news/a/why-this-risk-management-best-practice-is-not-fit-for-digital-innovation/

The first cluster '*support of top management'*, includes several aspects that have an effect on the way cyber risks are handled. The manner in which the leadership of an organization looks at the topic of risk management is an important factor in how seriously the entire organization regards this. In addition, the top of the organization can enable (or hamper) cyber risk leaders to successfully build out their teams and programs, which is of significant importance considering that cyber risk leaders create and drive the vision of what the cyber risk model should look like. Enabling the leaders of the cyber risk teams can be seen as a major factor when it comes to a successful implementation of some form of the Three Line Model. The '*Education*' cluster focuses on elements relating to the education of employees, emphasizing the importance of enhancing the knowledge of both the first and the second line. '*Contact and collaboration between teams'* embodies various elements relating to connections, in order to make the Three Lines Model a success. This can be by facilitating practical forms of contact, such as ensuring people are in the same room, or in the same time zone, and by ensuring that the right people are included in conversations between the business and the second line. Next to the practical forms of contact, it also includes more abstract forms of collaboration, for example the development of good relations between people. Here elements such as limiting hostility and building trust between teams are named. The fourth cluster '*organization structures*' looks at whether the impact of the existing structure of an organization can either support or negatively influence the success of second line knowledge in the first line. The responses to the interviews show that for instance a pillared company structure can lead to the splintering of risk appetite, with the unintended effect that different parts of the company may treat the same type of risk in a different way. Another point raised in the interviews about organization structures was that different maturity levels of an organization regarding cyber risk come with different structures around cyber risk management. More mature organizations are more likely to have a hybrid approach to privacy and security management, and usually there is an overall central knowledge hub, and decentralized cyber risk experts support different business teams separately. In less mature organizations a more centralized approach is often in place, as this is easier to scale up and less costly in terms of people and knowledge level.

The fifth cluster shows how '*Ownership'* can make a difference in supporting effective cyber risk management where second line knowledge is included in the first line. It highlights the impact of clear accountability in managing cyber risks. The last cluster, *'Transparency by digitizing',* is also an important issue when dealing with effective cyber risk management. An important effect of transparency is that it supports ownership, for example by having overview meetings or clear risk allocation via RACI models. Transparency can furthermore be enhanced by the use of relevant tooling and by digitizing cyber risk management where possible. This provides clear reports based on controls that are implemented and can facilitate conversations between the different lines. It was mentioned that tooling should not be used too early, when the organization is not mature yet.

The abovementioned points show that successful cyber risk management can be positively influenced by various elements, and that there is no one size fits all solution. When it comes to elements that support the Three Lines Model, companies must adapt these to their own context, in order to create an effective company approach for managing cyber risks.

8.4 Answering the research question

After answering the sub questions in the previous paragraphs, the research question can be addressed.
Can an approach where the traditional second line knowledge is brought into the first line lead to more effective management of cyber risks, and if yes, what elements are crucial for this approach to be successful?

Following the responses of the interviewees, we can state that in the experience of the respondents it is often the case that doing so can lead to more effective management of cyber risk. When asked, the interviewees often state that including second line knowledge into the first line, and thus creating a slightly modified version of the Three Lines Model, here named the Three Lines Bridge Model, contributes to more effective cyber risk management.

In addition to this we also see that information provided by answering the sub questions indicate that including second line knowledge into the first line solves several of the problems that are identified by interviewees when discussing challenges in cyber risk management following the Three Lines Model, as applied in their companies. When listing these problems, the key issues that were addressed are:

a. Lack in quality of communication between lines
b. Difficulties in creating accurate advice due to fast pace of technology and new laws
c. Limited ownership in the first line and fear of cyber risks
d. Long turnaround time of cyber risk processes

The benefits of including second line knowledge into the fist line led to:

i. Informed conversations & more accurate cyber risks
ii. Higher acceptance of cyber risks by the first line
iii. Improving turnaround time cyber risk reviews
iv. Including feedback loop for lawmakers

Below are some examples of how the application of I, ii and iii can lead to the reduction of concern in topics a, b, c and d. Point iv does not directly address the downsides of the Three Liens Model, however it can contribute to a better functioning ecosystem when better laws are created, thus impacting several of the downsides indirectly.

Benefit i*: informed conversation and more accurate cyber risks*, can be seen as a way to limit the impact of issue a. *lack of quality of communication between lines* and to some extend issue b. *difficulties in creating accurate advice due to fast pace of technology and new laws*.

Benefit ii: *higher acceptance of cyber risks by the first line* could be a way to (partially) address issue c. *limited ownership in the first line and fear of cyber risks*. The interviewees show us that ownership is enhanced when second line knowledge is brought into the first line, and when the first line better understands the risks that are flagged. This development may in part be amplified by benefit i: *informed conversations and more accurate cyber risks*.

Benefit iii: *improving turnaround time cyber risk reviews* addresses point d. *the turnaround time of the cyber risk processes*, as it shortens the time for the cyber risk review process.

Benefit iv: including feedback loop for lawmakers may indirectly address point b. *difficulties in creating accurate advice due to fast pace of technology and new laws*, as new laws may be easier to implement if the law was tailored to suit well to new technology. It may also indirectly address point d. *the turnaround time of the cyber risk processes*, as better tailored laws may lead to more straight forward requirements coming from the second line. However, further research on the effect of the feedback loop is recommended.

The above findings show that in the general opinion of the respondents and stemming from their experience and observations, including second line knowledge into the first line does not only lead to better cyber risk management, but it also shows which parts of cyber risk management will improve, and which specific issues are addressed or solved.

Taking the conclusion following the outcome of the interviews and analysis of the sub questions into account, this research shows that cyber risks are better managed when the Three Lines Model is modified into a hybrid '*Three Lines Bridge Model'* where second line knowledge is integrated into the first line.

This hybrid version of the Three Lines Model for tech-focused organizations is a logical next step from the initial Three Lines Model as described by the Institute of Internal Auditors. Where the Three Lines of Defense Model initially indicated a separation of the three lines, in its revision in 2020 and later in 2024 more space is created for potential collaboration between the first and second line. As, particularly in tech-focused companies, further building out this collaboration in a way that enables second line knowledge in the first line to be included has shown to be an important factor contributing to the success of the model, the Three Lines Bridge Model consolidates and anchors this even more so.

8.5 Limitations

Although this research has provided valuable findings, it also comes with certain limitations. These limitations are inherent to the type of research that was conducted, and to the research method used. The main limitations encountered during the research are listed below and these will be further elaborated upon. The main limitations includes the interview scope and focus, the literature that was reviewed and the time available for the research.

When choosing people to interview for this thesis, the emphasis was placed on finding people working in large organizations that have a strong focus on technology. As a consequence, the perspectives of other smaller companies, and organizations in different sectors was limited. For the scope of this research, this choice was a relevant one. However it would have been interesting to obtain insights from people working in different types of organizations and compare the results with the ones found in this thesis. This could provide more insights into whether the problems encountered with the Three Lines Model are specific to companies with a strong focus on technology and whether these findings can be found in other sectors as well. Similarly, it would be interesting to see if including second line knowledge into the first line would be beneficial in different sectors as well. Another limitation is the literature involved. Especially regarding (cyber) risk and the pacing problem, when a large amount of information is available. While a significant amount of literature has been studied for this thesis, there may be knowledge that was not included or missed out on. This is a result of the choices made, considering this paper is not a literature study and taking into account the time restraints. If

time had permitted, this thesis could have gone beyond the limits of the actual research and include a lot more in-depth information on topics such as the impact of ownership in (cyber) risk management and the Three Lines Model. It could also have included more information about how the third line, the governing bodies and the applicable external audit play a role in the effectiveness of the Three Lines Model for cyber risk management in tech-oriented companies. Below, in the 'Further research' section, we build on this limitation and discuss topics that were not addressed in this thesis but would be interesting to further investigate. Alas, this may be for another time, or another author.

8.6 Further research

Following the information gained in this thesis, several additional topics presented themselves, on which further research can provide more valuable insights. Some points where already raised in chapter 7, others are new and will be further elaborated on.

While reviewing the responses of interviewees on the downsides of the Three Lines Model, it appears that the issues around ownership and turnaround time for risks are present more frequently when applied to organizations with a strong focus on technology. It would be interesting to validate if this is the case, both through literature studies and by obtaining data on this topic, for instance by measuring cyber risk turnaround time in various types of organizations, or by verifying how many risks are mitigated in a certain time period. In this way we can establish if the examples and experiences of the interviewees align with what research in these organizations and the metrics involved show and draw further conclusions. Another point for further investigation relates to the involvement of the third line and other bodies mentioned in the model. As this document focuses on the first and second line, it excluded reviewing the impact of the other bodies in the Three Lines Model. However, for a more wholistic understanding of the benefits and downsides of the Three Lines Model in tech-oriented companies and the role the third line plays in this, it would be interesting to do further research on this.

Interviews show that ownership is crucial to enable effective cyber risk management in the Three Lines Model. Simultaneously it is frequently mentioned that enhancing ownership in organizations can be difficult. As a solution, bringing in second line knowledge into the first line, through the Three Lines Bridge Model, is proposed in this thesis. In addition to this solution, it would be valuable to identify if there are other factors that impact ownership, and what type of second line knowledge in the first line works best for different types of organizations. Local culture for example seems to impact ownership. As the culture in the Rhine area shows a stronger focus on the entire ecosystem and collective gains compared to organizations working in a Neo-American environment,[89] it could be that risk management and prioritization of risk mitigations are addressed differently. Whether there a differences between organization working in a Rhine paradigm compared to organizations working in a Neo-American environment when it comes to owning and mitigating risks could be valuable to investigate, as international organizations often operate in both environments. In addition, organizations in both environments can learn from each others approaches.

[89] Albert, M. (1993). *Capitalism against capitalism*. Four Walls Eight Windows. P18

Another challenge relating to ownership that transcends this thesis has to do with the moral responsibility of companies for the ethical choices they make. Today, we see that moral responsibility is an increasingly important topic in organizations.[90] The lack of clear rules in the digital domain poses the question: should everything that is not prohibited by law be allowed? A first line that only relies on the go/no go sign from the second line may lose the capability to make their own ethical decisions, which is even more important when it comes to new technology of which the early adaptions may become blueprints for our societies when adopting them. Just as there once were no laws prohibiting child labour in early day factories, or rules preventing chemical plants to dump their waste next to densely populated neighbourhoods, here too innovation may lead to behaviour that could be legal yet unethical. By not allowing the first line to think about the consequences of their creations, for example by only involving the Bridge 1.5 role in cyber risk management and not involving other parts of the first line, we may build an organizational framework where for people working in the first line contemplating about what 'the right thing' will be considered secondary to simply executing the norm that is set by the second line. It is therefore important to investigate the outcomes of the proposed model, and verify what over time, in the broader scheme of cyber risk management leads to the most desirable results.

To summarize this section about further research, it is recommended to review how the Three Lines Model is most effective in different environments when used for cyber risk management, and what long term effects are of the Three Lines Model and the proposed adjusted Three Lines Bridge Model.

9. Conclusions

This thesis started with a central research question:
Can an approach where the traditional second line knowledge is brought into the first line lead to more effective management of cyber risks, and if yes, what elements are crucial for this approach to be successful?

To answer this question, thirteen individuals working in organizations with a strong focus on technology have been interviewed in semi structured interviews. The individuals involved worked in different types of roles, varying in seniority from engineers and business managers to higher management and (supervisory) board members of organizations. This led to diversity in the responses.

The interviews taught us how the respondents perceive the application of the Three Lines Model in their organization. Most respondents recognized that the model, or important elements of it, were implemented in their companies cyber risk management structures. They also recognized that there were downsides to using the three lines model in their organization. Key topics amongst the things named were: a lack in quality of communication between the first and second line, difficulties in creating accurate advice due to fast pace of technology and new

[90] Gulati, R. (2023, November 22). Unifying your company around a moral goal. *Harvard Business Review*.

laws, limited ownership for cyber risks in the first line together with fear of cyber risks being flagged, and lastly the time it takes for cyber risk processes to be completed.

The thesis then looked at benefits of including first line knowledge into the second line. Following descriptions from interviewees, this can be done in various ways. For example by hiring employees with second line expertise to work in the first line as a so called '*bridge 1.5 role*', or via education of first line employees and champion structures. This adjusted implementation of the Three Lines Model, where first and second line knowledge is partially merged in the first line, is introduced in this thesis as the '*Three Lines Bridge Model*'.

The benefits of second line knowledge being brought in to the first line as described by respondents included: better (informed) conversations between the first and second line and more accurate cyber risks being flagged, a higher acceptance of cyber risks by the first line, an improvement of turnaround time for cyber risk reviews, and the inclusion of a feedback loop for lawmakers. When applying the Three Lines Bridge Model, several of the mentioned downsides to the Three Lines Model and the Three Lines of Defense Model could be resolved.

By better informed conversations and more accurately established risk cyber risks, the issue of lack in quality communication can be tackled, as well as, to some extend, the issue relating to difficulties in creating accurate advice due to the fast pace of technology and new laws. When there is a higher acceptance of cyber risks by the first line, struggles found around ownership will become less pronounced, and the downside of the model concerning the turnaround time is addressed as well, as the first line will be able to take requirements into account early on, preventing lengthy risk processes as they are mitigated or cancelled out before a second line review takes place.

These findings indicate that in essence, including second line knowledge into the first line can be beneficial for cyber risk management. This was confirmed by answers from interviewees when asked if they believe that including some form of second line knowledge into the first line could be beneficial. The majority of the respondents saw merit in this.

Some concerns were named as well, such as the large investment of including Bridge 1.5 roles in the first line, and the relevance or practicality of adding second line knowledge into the first line. Another point, raised specifically regarding the inclusion of Bridge 1.5 roles, is that this may take away from the responsibility and knowledge of the first line.

As this thesis looked at the experiences of interviewees, additional research is recommended to further investigate the effectiveness of the proposed Three Lines Bridge Model, and if it would also be effective in other type of organizations, and in other risk domains.

As our findings show, cyber risk management in tech-driven companies benefits from this more hybrid Three Lines Bridge Model. However, how each organization implements it will depend on their unique context and needs, as the model should be tailored in order to enable effective cyber risk management.

Literature list

Adam, B., Beck, U., & Van Loon, J. (2000). The risk society and beyond: Critical issues for social theory. SAGE Publications Ltd.

Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2022). The drivers of cyber risk. Journal of Financial Stability, 60, 100989. https://doi.org/10.1016/j.jfs.2022.100989

Ale, B. (2009). Risk: An introduction: The concepts of risk, danger and chance (1st ed.). Routledge. https://doi.org/10.4324/9780203879122

Allen, B. J., & Loyear, R. (2018). Enterprise security risk management: Concepts and applications (K. Noakes-Fry, Ed.; 1st ed.). Rothstein Publishing. Chapter 3.

Arnaud, A. (1662). La logique ou l'art de penser (p. 467).

Basel Committee on Banking Supervision, Bank for International Settlements. (2011). Principles for the sound management of operational risk. https://www.bis.org/publ/bcbs195.pdf

Basel Committee on Banking Supervision, Bank for International Settlements. (2014). Review of the principles for the sound management of operational risk. https://www.bis.org/publ/bcbs292.pdf

Bayuk, J. L. (2024). Stepping through cybersecurity risk management: A systems thinking approach. Wiley. https://doi.org/10.1002/9781394213986

Berg, B. van den, & Kuipers, S. L. (2022). Vulnerabilities and cyberspace: A new kind of crisis. Oxford Research Encyclopedia of Politics. https://doi.org/10.1093/acrefore/9780190228637.013.1604

Berg, H.-P. (2010). Risk management: Procedures, methods and experiences. Reliability: Theory & Application, 1(17), 80-81.

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. Geneva Papers on Risk and Insurance - Issues and Practice, 40(1), 131–158. https://doi.org/10.1057/gpp.2014.19

Brender, N., Gauthier, M., Morin, J.-H., & Salihi, A. (2024). Three lines model paradigm shift: A blockchain-based control framework. Journal of Applied Accounting Research, 25(1), 149–170. https://doi.org/10.1108/JAAR-06-2022-0143

Brumfield, C. (2022). Cybersecurity risk management: Mastering the fundamentals using the NIST cybersecurity framework. John Wiley & Sons, Inc. https://doi.org/10.1002/9781119816348

Cebula, J. L., & Young, L. R. (2010). A taxonomy of operational cyber security risks.

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. The Geneva Papers on Risk and Insurance - Issues and Practice, 47(3), 698-736. https://doi.org/10.1057/s41288-022-00266-6

European Commission. (n.d.). Europe fit for the digital age. Retrieved from https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en

Gellert, R. (2020). The risk-based approach to data protection. In Oxford Data Protection & Privacy Law (online edn). Oxford Academic. https://doi.org/10.1093/oso/9780198837718.001.0001

Giddens, A. (1999), Risk and Responsibility. The Modern Law Review, 62, p1-5 https://doiorg.ezproxy.leidenuniv.nl/10.1111/1468-2230.00188.

Gulati, R. (2023, November 22). Unifying your company around a moral goal. *Harvard Business Review*.

Huibers, S. C. J. (2015). Combined assurance: One language, one voice, one view. The Institute of Internal Auditors Research Foundation. Available at: https://perma.cc/D7YM-9GS

Johnson, W. G. (2022). Caught in quicksand? Compliance and legitimacy challenges in using regulatory sandboxes to manage emerging technologies. Regulation & Governance.

Krumay, B., Bernroider, E. W. N., Walser, R., & Gruschka, N. (2018). Evaluation of cybersecurity management controls and metrics of critical infrastructures: A literature review considering the NIST cybersecurity framework. In Secure IT Systems (Vol. 11252). Springer International Publishing AG. https://doi.org/10.1007/978-3-030-03638-6_23

Luburić, R. (2017). Strengthening the three lines of defence in terms of more efficient operational risk management in central banks. Journal of Central Banking Theory and Practice, 6(1), 29–53. https://doi.org/10.1515/jcbtp-2017-0003

Moerel, L. (2020). Why this risk management best practice is not fit for digital innovation. IAPP. https://iapp.org/news/a/why-this-risk-management-best-practice-is-not-fit-for-digital-innovation/

Mukhopadhyay, A., Saha, D., Mahanti, A., Chakrabarti, B., & Podder, A. (2005). Insurance for cyber-risk: A utility model. Decision, 32, 156-157.

Saudi Authority for Data and Artificial Intelligence. (2021). Personal Data Protection Law (Article 29 and Article 32).

Saudi Authority for Data and Artificial Intelligence. (2023). Personal Data Protection Law (Version 2) (Article 29 and Article 32). Retrieved from https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal%20Data%20English%20V2-23April2023-%20Reviewed-.pdf

Saudi Authority for Data and Artificial Intelligence. (n.d.). Personal Data Processing Activities Records Guideline. Retrieved from https://sdaia.gov.sa/Documents/PersonalDataProcessingActivitiesRecordsGuideline.pdf

Schuett, J. (2023). Three lines of defense against risks from AI. AI & Society. https://doi.org/10.1007/s00146-023-01811-0

Schwartz, B. (1994). On morals and markets. Criminal Justice Ethics, 13(2), 61. Retrieved from https://login.ezproxy.leidenuniv.nl/login??url=https://www.proquest.com/scholarly-journals/on-morals-markets/docview/1297908397/se-2

Secureworks. (2024). Boardroom cybersecurity report 2024. Retrieved January 17, 2025, from https://www.secureworks.com/centers/boardroom-cybersecurity-report-2024

Seidenfuss, K.-U., Young, A., & Datwani, M. (2023). Integrating governance, risk and compliance? A multi-method analysis of the new Three Lines Model. SN Business & Economics, 3(10). https://doi.org/10.1007/s43546-023-00561-x

Slapničar, S., Axelsen, M., Bongiovanni, I., & Stockdale, D. (2022). A pathway model to five lines of accountability in cybersecurity governance. University of Queensland.

Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. International Journal of Accounting Information Systems, 44, 100548. https://doi.org/10.1016/j.accinf.2021.100548

Statista. (2024). Cybersecurity worldwide. Retrieved January 17, 2025, from https://www.statista.com/outlook/tmo/cybersecurity/worldwide

Stibbe. (2023). EU Artificial Intelligence Act and Generative AI: An Update. Retrieved from https://www.stibbe.com/publications-and-insights/eu-artificial-intelligence-act-and-generative-ai-an-update

Taeihagh, A., Ramesh, M., & Howlett, M. (2021). Assessing the regulatory challenges of emerging disruptive technologies. Regulation & Governance, 15(4), 1-2.

The Institute of Internal Auditors. (2013). The three lines of defense in effective risk management and control. The Institute of Internal Auditors. Available at: https://theiia.fi/wp-content/uploads/2017/01/pp-the-three-lines-of-defense-in-effective-risk-management-and-control.pdf

The Institute of Internal Auditors. (2020). The IIA's three lines model: An update of the three lines of defense. The Institute of Internal Auditors. https://www.theiia.org/globalassets/site/communication/2020/three-lines-model-updated.pdf

The Institute of Internal Auditors. (2024). The IIA’s three lines model: An update of the three lines of defense. Retrieved from https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf

Valkenburg, B., & Bongiovanni, I. (2024). Unravelling the three lines model in cybersecurity: A systematic literature review. Computers & Security, 139, 103708. https://doi.org/10.1016/j.cose.2024.103708