FACULTY OF SCIENCE AND TECHNOLOGY

MASTER'S THESIS

Study programme / specialisation: Risk Analysis and Governance	The *spring* semester, *2023* Open
Author: Aliya Vogt Pomerantz	
Supervisor at UiS: Terje Aven	
Thesis title: A comparative analysis of security risk management in Norwegian oil and gas and renewable energy companies.	
Credits (ECTS): 30	
Keywords: Renewable production, Security risk, Risk Governance, Security Risk Assessments, risk tolerability	Pages: 76 + appendix: 86 Stavanger, *15.06.2023*

Master Thesis 2023

Faculty of Technology & Science

Supervisor: Professor Terje Aven

A comparative analysis of security risk management in Norwegian oil and gas and renewable energy companies.

An investigation on how energy companies can manage security risks in a cost effective and commercially viable context for their future renewable energy portfolios.

Aliya Vogt Pomerantz

MSc Student Risk Analysis & Governance

University of Stavanger

Abstract

With the recognised urgent need to combat climate change globally, the renewables industry has witnessed significant growth to meet ambitious net zero targets. This thesis aims to emphasize the importance of improving security risk governance to adapt to the evolving energy sector. The increasing adoption of renewable solutions and the expansion of renewable production presents a landscape characterized by uncertain and complex market dynamics. Additionally, these developments contribute to a more adverse threat environment driven by innovation in research and development (R&D), technology, and digitalization. Considering these advancements, criminal actors now have greater opportunity, motive, and increased capabilities, regardless of whether the company is focused on oil and gas, or renewable production. While damages to a renewables asset result in lower costs and less detrimental environmental impacts when compared to an offshore oil and gas asset, they can still have adverse implications on company values. Impacts to critical renewable assets have the potential to increase reliance on traditional fossil fuels, negatively impact local communities, and detrimentally impact company margins. Furthermore, due to market volatility and energy politics, nations aim to safeguard energy supply and reduce dependence on external sources. This is particularly relevant when considering the sanctions imposed on Russian oil and gas following the 2022 invasion of Ukraine. As a result, energy independence and energy security have become increasingly more critical.

This thesis has identified with certainty that there is a significant lack of maturity within security risk governance in renewables companies. Therefore, by comparing how both the oil and gas, and renewables sector acknowledge security and therein approach security risk management, a platform is created to offer fit-for-purpose recommendations to the renewables sector. Furthermore, this thesis acknowledges the lower margin nature of renewable production and ultimately emphasises fostering a sustainable and dynamic security culture that allows industry to strategically expand into higher security threat environments.

Key words: Renewable production, Security risk, Risk Governance, Security Risk Assessments, risk tolerability

Foreword

I want to take this opportunity to sincerely thank my supervisor, Professor Terje Aven at the University of Stavanger for his steadfast support, guidance, and patience. Without your constructive criticism, words of wisdom and constant reliability throughout this process, this thesis would not have been possible.

I would also like to thank Anders Rimstad and Aina Slinning at Aker ASA, Nicholas May at Aker Solutions, and Ronny Løvbakke at Aker BP for taking the time to share their invaluable knowledge and expertise on security risk management with me. Furthermore, I would like to extend my gratitude to Charles Winge-Main at Equinor for illuminating issues surrounding the security risk management of renewable energy production. Without your initial guidance and our insightful conversations, this thesis would not have come to light.

Finally, I would like to express my immense gratitude to my wonderful parents for their constant love and support throughout my life and academic career. Although you are many thousands of kilometres away, you were always a phone call away when I needed you the most.

Aliya,
2023

Table of Contents

Abstract 1

Foreword 2

List of Abbreviations 6

List of Figures 7

List of Tables 7

Chapter 1 8

Introduction 8

1.1 Background 8

1.2 Purpose of thesis 9

1.3 Contents 10

1.4 Methodology and approach 10

Chapter 2 12

Analysis of renewable market factors and their correlation to uncertain and complex risks 12

2.1 The four risk problem categories 13

2.1.1 Overview of simple, uncertain, complex, and ambiguous risk 13

2.1.2 Deciding upon the appropriate management strategy 16

2.2 Renewable markets as uncertain and complex risk 16

2.2.1 Global market risks and opportunities 17

2.2.2 Company renewable market landscape 21

2.3 Closing remarks on risk type correlation and company landscape 27

Chapter 3 28

Security comparisons 28

3.1 Company risk practices and SRA processes 29

3.1.1 Comparing reported security practices between the companies 29

3.1.2 Comparing SRA methods between the companies 33

3.2 Comparing threat type categories 37

3.2.1 Threat category information 38

3.3 Comparing impact categories 42

3.3.1 Impact category information 42

3.4 Comparing threat actor capability and intent categories 44

3.4.1 Threat actor category information 46

Chapter 4 48

Discussions 48

4.1 Appropriate risk management tools (for uncertain & complex risk) 48

4.1.1 Cautionary/precautionary based management strategies 51

4.1.2 Risk-informed management strategies 55

4.2 Company risk appetite and tolerability 58

4.2.1 Aker Horizons (Mainstream RP) 59

4.2.2 Aker Solutions 60

4.2.3 Aker BP 61

4.3 Suggested improvements to renewable security practices 62
4.3.1 Aker Horizons (Mainstream RP) 62
4.3.2 Aker Solutions 64
4.3.3 Closing remarks on suggested improvements 65
Chapter 5 67
Conclusion 67
Appendixes 71
Appendix A 71
Company renewable market landscape 71
In-text citations for Table 1 75
Appendix B 76
Reporting summaries of security practices between the companies 76
Appendix C 80
Interview transcript 80
References 81

List of Abbreviations

(A, C, U)	Risk definition: A: Activity/event(s) occurring C: Consequences given A U: Uncertainty regarding C
ALARP	As Low As Reasonably Practicable
CCUS	Carbon Capture Utilisation and Storage
CIF	Climate Investment Fund
ENPV	Expected Net Present Value
ERM	Enterprise Risk Management
ESG	Environmental, Social, Governance
GHG	Greenhouse Gas
HSSE	Health Safety Security Environment
IDD	Integrity Due Diligence
IPG	International Partners Group
IRGC	International Risk Governance Council
IT	Information Technology (cyber)
NIST	National Institute of Standards and Technology
OT	Operational Technology
PPA	Power Purchase Agreement
R&D	Research and development
RP	Renewable Power
SRA	Security Risk Assessment
SoK	Strength of Knowledge
TCFD	Task Force on Climate-related Financial Disclosures
USAID	U.S. Agency for International Development

List of Figures

Figure 1 Threat actor capability & prevalence scale for Aker ASA (Aker ASA, 2022) 45
Figure 2 ALARP outline. Adapted from Aven (2014); Abrahamsen & Abrahamsen (2015) 54
Figure 3 Layered approach to ALARP (Aven, 2011, p. 9) 55
Figure 4 Suggested methodology for knowledge assessment (Sørskår et al., 2019) 57

List of Tables

Table 1 Market landscape concerns for the listed countries 23
Table 2 Company security focus areas 29
Table 3 Company security standards & frameworks 30
Table 4 Company security risk management tools and practices 30
Table 5 Company security-focused business areas & systems 32
Table 6 Company key security developments 32
Table 7 Comparing identified threats between the companies 38
Table 8 Comparing identified impacts between the companies 42
Table 9 Comparing identified threat actors between the companies 45
Table 10 Management strategies for uncertain risk (Based on Aven 2014, p. 164) 50
Table 11 Mainstream Renewable Power – Europe Market Landscape 71
Table 12 Mainstream Renewable Power – Latin America Market Landscape 72
Table 13 Mainstream Renewable Power – Africa Market Landscape 72
Table 14 Mainstream Renewable Power – Asia Pacific Market Landscape 73
Table 15 Aker Solutions – Global Market Landscape 74

Chapter 1
Introduction

1.1 Background

The inception of this thesis was motivated by discussions pertaining to the evolution of security culture within the energy sector in Norway. These conversations with safety, security and sustainability experts working in Norwegian oil and gas, and renewables, illuminated the role security has played from the events of September 11th, 2001, and more recently following the direct attack on the energy sector at In Amenas, Algeria in 2013, where 40 individuals lost their lives. It was highlighted that following these events, security risk management in the oil and gas sector was ultimately strengthened, creating an increased security awareness across the industry. Conversely, as the energy industry transitions into renewable solutions, there is a growing awareness among energy companies on the lack of security risk research, competence and focus concerning renewable power and associated assets.

As a response to the climate crisis and the goal of achieving net zero targets by 2050, in accordance with the recommendations by the IPCC (Intergovernmental Panel on Climate Change), there has been a significant acceleration in global investments toward renewable technologies. Consequently, the energy sector is undergoing a challenging transition from traditional fossil-fuel energy sources towards sustainable and low-carbon alternatives. This increase in renewables and the radically different business model means that broad energy companies must rethink their risk management principles and processes to meet these new realities. Furthermore, as renewables start to play a more critical role in energy production, they also become increasingly more attractive targets to hostile actors. To succeed with the energy transition and adapt to the challenges of a fast moving and lower margin business, increased focus towards adapting governance will be necessary.

In order to address security risk deficiencies and promote the adaption of governance within renewable production, this thesis provides an analysis of risks pertaining to market challenges

and a comparison of security practices across the oil and gas, and renewable sectors. Risk, in this thesis, is broadly defined as the consequences (C) of an activity (A) and associated uncertainties (U); (A,C,U) (Aven & Thekdi, 2021, p. 11). Market risks are specified when analysing the energy transition, as energy majors face significant challenges in terms of the at present low margin context. Energy companies, which have predominantly operated in low to medium physical security threat locations may benefit from operating in new geographies with higher security threats to find higher margin opportunities. In lieu of new geographies, there are different risks and threat categories correlated with political climates, policies and regulations, economic constraints, and having to balance the ongoing competition from oil and gas. This poses questions on risk and reward if security mitigation costs negatively impact profitability, and whether businesses will ultimately need to tolerate and carry higher residual risk. With the consensus of achieving net zero by 2050 - and for many companies engaging in renewable production, to secure assets by 2030 - it is the author's motive to take into account the difference of scale in investments, margins, and security threats between the oil and gas, and renewable sectors. Therefore, by creating an overview of relevant market and physical risks, necessary steps towards creating awareness and universality within the security risk management of renewables can take place. This will be significant when securing new technologies as well as protecting assets of critical national infrastructure that will assist in the energy transition.

1.2 Purpose of thesis

This thesis has three main objectives. Firstly, to deepen understanding of the uncertain and complex market challenges faced by renewable production in various geographies of operation. Secondly, to gain a better understanding of the security risk culture within renewables companies, the current security risks renewables companies face, and the methodologies they utilised to assess and manage security risk. Finally, by analysing these elements, this thesis can then assist renewables companies in evaluating the effectiveness, adequacy, and deficiencies of current security practices. This will allow the author to design and offer fit-for-purpose recommendations in accordance with the evolving nature of both the energy sector and the security landscape. Using this approach will provide an overview of the risks renewable

companies face and incentivise companies to operate strategically while also tolerating risk in a lower margin context in higher security threat environments.

1.3 Contents

This thesis is structured as follows: Chapter 2 will present the linkage between renewable market factors and how these fit into the uncertain and complex risk category. The relevant market challenges and the specific risks and opportunities correlated with renewable production will be discussed in view of the locations in which the analysed companies currently have or plan to have operating assets. Chapter 3 will present a comparison of available data on company security risk processes and assessments, coupled with an analysis of recognised security threat, impact, and threat actor intent categories between the analysed companies. Data is collected using annual and sustainability report analyses as well as interviews from heads of security within the companies. Chapter 4 will first interpret the results obtained through the market analysis in chapter 2 to provide suggestions on fit-for-purpose tools and measures, which can be utilised in future renewable security risk assessments (SRA). Secondly, expert perception on risk tolerability will be analysed to determine how much residual risk the companies are currently accepting. Understanding tolerability will help pave the way for assessing and implementing appropriate security practices. Finally, suggested improvements to renewable security practices will be offered in light of company analyses. Chapter 5 concludes the thesis by elaborating on the significance of main findings and suggested directions for future research in the field.

1.4 Methodology and approach

This thesis is a qualitative and descriptive evaluation of the market and security risks associated with the increase in renewable production, as well as an analysis of renewable sector security practices compared to oil and gas. Moreover, this thesis assesses the types of tools and measures that can be useful in application to combat the analysed risks. The objectives of this thesis are attained by considering three different Norwegian energy companies, operating within the renewable and oil and gas sectors, and their approaches to evaluating and assessing security risks.

Academic knowledge regarding risk management is sourced from relevant literature, and courses pertaining to risk analysis and governance from the University of Stavanger. Company knowledge is sourced from Aker ASA (investment company) and subsequent portfolio companies, including Aker BP (oil and gas production), Aker Solutions (oil, gas, and renewables engineering), Aker Horizons (renewable production and subsidiary investment company), and Mainstream Renewable Power (portfolio company to Aker Horizons). This thesis does not include data sampling or participants in a formal capacity.

As this thesis focuses on renewable market risks and malicious security risks, excluded completely or from in-depth analysis includes but is not limited to the following risks: workplace safety and health risks; financial and related risks such as currency, credit, and liquidity risks; bribery and corruption risks; human rights related risks; oil and gas market risks; and other external risks such as Covid-19 and physical environmental or weather-related risks. Contextual mention of the above may be necessary, but it is not the focus of this thesis.

Chapter 2
Analysis of renewable market factors and their correlation to uncertain and complex risks

The global renewable energy market is rapidly evolving, impacted by and reacting to numerous interrelated factors that dynamically affect its development. The renewable energy market is analysed in order to account for variations in geopolitical and bureaucratic processes across regions with different levels of natural resource availability. The relevant factors affecting the successful procurement, production, and protection of renewable energy depends greatly on the interactions between political climates' policies and regulations, economic conditions and constraints, technological advancement, competition from oil and gas, as well as accepted forms of energy within a given region. Due to these factors, the production of renewable energy can be defined within the categories of uncertain and complex risk when compared to the market maturity and returns on investment associated with oil and gas. To navigate the uncertain and complex factors correlated with the growth and the rapidly evolving renewable energy market, geographical considerations pertaining to security risks will be analysed in accordance with the IRGC (International Risk Governance Council) Risk Governance Framework (2005). This framework acknowledges a distinction between four classes of risk, including simple (linear), uncertain, complex, and ambiguous risk problems. The objective of analysing these risk problems in the context of market risks is to facilitate discussion in chapter 4 on the appropriate management approach, including relevant tools and measures to support the growth and protection of renewable production.

In this chapter, the analysis will first focus on distinguishing between the four types of risk problems, drawing attention to why market risks associated with renewable production are placed under the uncertain and complex category. Step two will examine relevant market challenges and the specific risks and opportunities linked to renewable production. This will then be complemented by an outline of the renewable market landscape of the analysed portfolio companies, identifying where the companies have assets and the relevant market risks in those locations.

2.1 The four risk problem categories

Understanding the different types of risk problems relating to renewable energy production and energy markets will have a ripple effect on how risk is identified, judged, and managed. In Renn (2017), the author discusses three categories of management approaches associated with the four classes of risk problems, namely, the risk-informed management approach, cautionary/ precautionary approach (resilience-oriented), and the discourse-oriented approach. These options were devised in line with the IRGC Risk Governance Framework (2005), to support the development of appropriate risk management instruments and tools associated with simple, uncertain, complex, and ambiguous risk problems. Renewable energy production and markets are understood as uncertain and complex risk problems, although chapter 2.1.1 will distinguish between the four risk categories to support the above claim. Chapter 4 will go on to discuss the appropriate management approach associated with uncertain and complex risk. The following overview of risk is built on IRGC (2005) and Renn (2017) concept of risk governance, while acknowledging updated input from Aven and Renn (2020).

2.1.1 Overview of simple, uncertain, complex, and ambiguous risk

Simple Risk

In short, a simple risk is one where the occurrence and associated consequences of an event can be predicted quite accurately (Aven & Renn, 2020). This type of risk can use probabilistic analyses to assess risks and consequences with predictable or non-random structures. For example, the risks correlated with the act of smoking are understood as simple risks.

Uncertain Risk

With uncertain risks, there is no clear consensus on how to predict the occurrence of uncertain events and their consequences. An example of uncertain risk is the event of terrorism and the type of attack, although the consequences can to an extent be predicted (Aven & Renn, 2020). In the case of terrorist attacks, there is often incomplete and varying data on the analysed risk. Another example includes the risks pertaining to market challenges and renewable production,

which are further understood as epistemic uncertainty**,** as there is a lack of knowledge within the fundamental phenomena.

Uncertainty can be reduced by generating more knowledge, although, historical data and statistical analysis are often a weak source of knowledge, as context changes with each event. Uncertainty can be expressed using knowledge-based (subjective) probabilities, which can be expressed through a Bayesian Analysis. All probabilities are contingent on background information, available data, and the models used. It is advised that a cautious strategy is followed, which allows for learning by restricted errors (Renn, 2017). The overarching goal when managing uncertain risks associated with renewables is to create a resilient system for production to thrive, capable of combating unpredictable events connected to market challenges and security breaches.

Complex Risk

Complex risks are often correlated with the performance of an individual component within a large complex system. There is limited relevant data on the effect of a singular component within the system and how the system as a whole will react to its application or discontinuity (Aven & Renn, 2020). The source of the risk (risk agent) may cause contention, leading to uncertainty regarding the observed effects of an individual component. This can cause issues when implementing appropriate safety measures to combat vulnerability. Thus, complex risks are a special case of uncertain risks. Ultimately, there is difficulty in identifying and quantifying the relationships between the source of the risk and the magnitude of the observed consequences. This type of risk is particularly prevalent in new technologies, such as those associated with new low carbon solutions, as well as within systems related to critical infrastructures (Aven & Renn, 2020).

Increasing knowledge is necessary to decrease contention and or uncertainty. Suggested methods for increasing knowledge in the context of this thesis may include conducting threat analyses concerning geography, taking into account known malicious actors or evidence of unrest. Furthermore, appropriate measures taken to improve buffer systems may be necessary, which may include increased safety and redundancy measures. If the knowledge obtained leads to the

conclusion that there is heightened uncertainty, uncertain risk strategies will be useful in application. This links to the interlacing system, connecting the management strategies for the specific risk problem (Renn, 2017), which will be discussed further in chapter 4.1. If the risk agent is already known and there is limited uncertainty, creating a robust system capable of withstanding shock will be applicable.

Ambiguous risk

Renn (2017) considers two types of ambiguous risk: Interpretive ambiguity and normative ambiguity, both of which are often the result of uncertain and complex risks.

Interpretive ambiguity concerns risk with inconclusive (weak) knowledge, little consensus on consequences, and competing evidence or interpretations, but not on values. These conditions lead to large uncertainties and a potential for significant consequences. For example, in a scenario where there is lack of consensus on which renewable technology option to pursue, uncertainty or competing evidence can apply to the relevant trade-offs between technologies. Such trade-offs can be linked to the success and cost-effectiveness of production. In this scenario, interpretive ambiguity may be caused by misinterpretation of the specific risk problem and therefore its associated consequences. This may lead to miscommunication on appropriate risk measures, resulting in poor investment decisions and inferior climate mitigation efforts.

Normative ambiguity according to Renn (2017) pertains to risk with inconclusive or ambiguous values but not evidence. Aven and Renn (2020) go on to state that normative ambiguity reflects the fact that there are different views regarding “the values to be protected and the priorities made…” (p. 4). It is less about “interpretation but how one gives weight to different concerns” (p. 8). This is exemplified when considering the implementation of nuclear energy as a renewable solution to climate change. The risks correlated with this technology are scientifically understood, but the perception and weight towards relevant benefits, concerns and uncertainties, vary (Aven & Renn, 2020).

In conclusion, while "the three other categories reflect features related to knowledge about the activity considered…normative ambiguity concerns how we like/dislike or value these features. Thus, normative ambiguity extends beyond the scientific domain" (Aven & Renn, 2020, p. 8).

2.1.2 Deciding upon the appropriate management strategy

Uncertain, complex, and ambiguous risk problems can be characterised as systemic in nature. In the context of this thesis, market risks are systemic as they affect operations as a whole. Such risks include changes in governing policies, weather events, financial crises, and pandemics, which can impact the distribution of energy. In the case of combating systemic risks, policy and regulation impacts the success or degradation of the system. On the other hand, security threats pertaining to renewable production are systematic, as the effect is directed at individual parts of the system. Conversely, in a safety context, systematic risk could be associated with equipment malfunction, and would rather require targeted technological or operational solutions instead of broad regulatory changes.

By identifying that renewable production and associated market risks are uncertain and complex, as well as systemic and systematic, appropriate risk management strategies can be used to align with these factors. This approach is in line with IRGC Risk Governance methods and reaches beyond the probabilistic analysis strategies suited towards simple risk problems (Aven & Renn, 2020). Further discussion of these risk management frameworks and tools will be discussed in chapter 4.

2.2 Renewable markets as uncertain and complex risk

Chapter 2.2.1 will evaluate in-short which specific market factors create uncertain and complex risks with renewable energy production, including any opportunities tied to these factors. In summary, chapter 2.2.2 will introduce where the Aker companies have or consider developing assets and the specific challenges (uncertain and complex risks) they face regarding the locations in which they operate.

2.2.1 Global market risks and opportunities

Listed below are a non-exhaustive list and brief account of relevant global renewable market influences and their impacts. Impacts are acknowledged as both the risks and opportunities that they pose to renewable energy companies' development agenda. These market parameters discuss in short, the issues of regulatory frameworks, financial uncertainties, technology advancements and geopolitical climates, and how they impact renewable production and, therefore, the speed of the energy transition. These parameters are obtained primarily from analysing recent documents and organisational reports associated with Aker Solutions, Aker Horizons and Mainstream Renewable Power (at times abbreviated to Mainstream RP).

Policy and regulatory impacts on the speed of the energy transition

In environments where favourable renewable energy policies are prioritised, the energy market is given greater leeway to transition from fossil fuels to sustainable options. The significant uncertainties regarding long-term changes in subsidies, regulations, and carbon pricing are, therefore, considered a prioritised risk focus by Aker Solutions (The Governance Group AS, 2021). When considering Mainstream RP, the markets in which the company has operated in as of 2021, have been characterised as growth markets with high levels of market and regulatory uncertainty. Growth markets, such as the renewable production sector, are inherently prone to uncertainty owing to the dynamic nature of factors like rapidly changing conditions, the emergence of new competition, and the ongoing evolution of regulations. Specifically, uncertainties with climate change mitigation regulations significantly impact the functions of supply and demand for renewable technology and advancement. Aker Horizons tackles the issue of market volatility concerning regulatory development by engaging heavily in public policy both internally and externally. In terms of government support, regulatory supply incentives can, in many cases, take the form of Feed-In Tariffs, which can encourage the deployment of renewable technology and utilities, thus incentivising investment and increasing supply to the renewable energy market (Sandeman, 2010). In terms of demand, there is general uncertainty regarding the pace of change in demand for renewable technology and services. Aker Solutions considers this to be an additional main risk factor (The Governance Group AS, 2021).

Among the regulatory incentives considered effective at combating these issues are carbon tax policies and quota obligation systems. Quota obligation systems require a percentage of energy flowing into the market to be from renewable resources, thus increasing demand. These renewable obligation systems, or RO, in the United Kingdom, are known as Renewable Portfolio Standards (RPS) in the United States and Renewable Energy Targets in Australia (de Arce & Sauma, 2016). Quota systems are considered the most cost-effective policies at reducing CO_2 emissions, specifically in the context of a perfectly competitive energy market. However, if the electricity market is not perfectly competitive, quota systems are still as effective if subsidies are directly paid back through electricity tariffs unless the cost of renewable energy significantly drops. Ultimately, it is prudent to note that the efficacy of regulatory incentives and industrial policies depend on the cost of the specific renewable technology, coupled with the current market structure and an analysis of how subsidies impact customers (de Arce & Sauma, 2016).

Operating in countries which incentivise these regulatory practices is beneficial, although delays in construction and production can still occur if the country of operation experiences unpredictability associated with regulatory setbacks. For the Aker portfolio companies to gain market acceptance, minimise licensing, permitting and consenting delays and ultimately reduce operational costs, the companies will require favourable and predictable regulatory environments (Aker Horizons ASA, 2023). Opportunistically, Mainstream RP invests in many different locations, with most assets operating in locations which support optimal renewable legislation. This does not go without mentioning that Aker Horizons as the subsidiary investment company, is still exposed to project execution risks related to key suppliers, sub-suppliers, grid availability, and permitting challenges. These challenges are coupled by extraneous market risks, which may delay actualisation of policy implementations (Aker Horizons ASA, 2023). In the short term, Aker Solutions has identified regulatory opportunities associated with a clear and consistent regulatory framework for carbon taxing on oil and gas up to 2025, furthermore, 2022 saw an increase in new climate-positive policy announcements (The Governance Group AS, 2021). Optimistically, green policy is advancing exponentially, with the IEA (International Energy Agency) reporting renewables to account for over 90 percent of the global electricity increase within the next five years (Aker Horizons ASA, 2023).

Financial uncertainties

In countries which experience the underdevelopment of renewable energy, high initial capital costs of development are seen as a contributing obstacle to the growth of renewable production. The speed of the energy transition will ultimately be quicker in countries with well-developed financial markets as they have greater access to external financing (Kim & Park, 2016). Regions experiencing higher costs of energy will have greater incentives to invest in energy, whereas regions and processes requiring energy input (such as the production of hydrogen and green steel) need greater policy support (Aker Horizons ASA, 2023). Furthermore, the limits on margins or returns on investment concerning renewable energy compared to oil and gas act as an additional hindrance, especially with the added costs associated with inflation, supply chain disruptions, and interest rate increases (Aker Horizons ASA, 2023, p. 24). The cost and access to consistently larger amounts of capital are considered a high and increasing risk, as procurement is demanding and at times unstable (Aker Horizons ASA, 2022, pp. 25, 191). Long-term financing schemes will be necessary for the development of the renewables sector and to combat the issue of a competitive, low-margin market, which experiences levelized cost increases.

Furthermore, financial uncertainties can be expedited if the company is exposed to detrimental reputational risks. With renewable energy companies such as Mainstream RP or Aker Solutions being connected to the fossil fuel industry, external partnerships, goodwill, and recruiting could be negatively impacted. This, although is considered a low level risk when compared to the reputational opportunities and growth related to climate positive initiatives and local community incentives, both of which are likely to attract greater investment opportunities and a younger workforce, in contrast to oil and gas companies (Mainstream Renewable Power, 2022); (Aker Horizons ASA, 2023); (Aker Solutions ASA, 2022a).

Aker Horizons as a subsidiary investment company, relies on functioning debt and equity markets to fund their renewable portfolio. The company manages the finances of its portfolio companies, including Mainstream RP by maintaining solid liquidity reserves. This is achieved by both Aker Solutions and Aker Horizons proactively planning refinancing activities as well as diversifying funding sources (Aker Horizons ASA, 2023); (Aker Solutions ASA, 2023d). As

stated, the Aker companies will benefit from developing renewable energy within countries, which support climate positive policy initiatives, making access to financing easier for renewables focused energy companies. An issue to consider is the natural resource availability within countries with both lower and greater access to financial incentives. Energy resources and green policy are unevenly distributed across the globe, where certain less-developed countries may have greater resource availability, but poorer market capacity. With the demand for energy increasing, renewable energy companies will benefit in the short term by continuing asset, technology, and revenue diversification into markets supported by the energy transition (The Governance Group AS, 2021). Ultimately, companies will benefit from incentivising competency growth, and to the best of their abilities, developing resilient assets within locations which already incentivise renewable production. In the long term this will improve energy security within a given nation, while also allowing for the global energy market to mature.

Technological advancements and renewable development

Lack of green infrastructure maturity creates uncertainty when developing renewable technology in less developed locations and thereby creates challenges in producing adequate amounts of energy. Infrastructure maturity may be in the form of pipelines, access to the grid, and battery storage, among others. Furthermore, operational uncertainty and risk include those where a company, such as Aker Solutions, is able to successfully commercialise new technology within a given location that has traditionally used other forms of energy (Aker Solutions ASA, 2022a). Positively, demand for renewable technology is increasing, thus introducing greater market opportunity. This is specifically notable in carbon capture and offshore wind farm installations.

Geopolitical instability risks (political climate)

Civil and political unrest can cause unpredictability, uncertainty, and disruption to the global economy and supply chain within the market system. In the case of energy markets, this can lead to delays in construction and production, as well as result in increased reliance on traditional fossil fuel energy sources. The 2022 Invasion of Ukraine is among the most recent developments in geopolitical instability, from which sanctions against the import of Russian energy have caused extensive business and global market uncertainty and disruptions. Uncertainty is associated with the timeframe in which the war will last and how Russian sanctions will continue

to impact the supply chain and increasing energy demand. This spurs the debate on energy security and the growing need for energy independence in Europe, where individual nations will benefit from realigning policy to take advantage of their own natural resources. Other examples of geopolitical strain on resources and business operations include global pandemics. Continually monitoring developments of geopolitical instability are necessary to mitigate impacts, where possible. In 2021, Mainstream RP managed increased costs and constraints to the supply chain from geopolitical instability by continuously focusing on cost discipline and diversifying sourcing approaches (Aker Horizons ASA, 2023, p. 18).

2.2.2 Company renewable market landscape

The renewables companies used for landscape assessment are Mainstream RP and Aker Solutions. This subchapter will disclose the locations in which the companies have or consider developing assets. This data will support in connecting the uncertain and complex market factors associated with renewable energy production within these locations. Chapter 3 and 4 will further discuss security risks linked to these locations. Company location data in Table 1 is obtained via the 2021 and 2022 Mainstream Renewable Power Sustainability Report, the 2021 and 2022 Aker Solutions Sustainability Report, and company websites. Geographical information in Table 1 is obtained via online government or company websites, official energy websites and academic articles.

Only asset and potential asset locations as indicated by Mainstream RP and Aker Solutions will be analysed and listed. Office locations will not be included. Specified Mainstream RP locations include Europe (Norway, Sweden, UK, Ireland), Asia Pacific (Australia, Vietnam, Philippines, South Korea, Japan), Latin America (Chile, Colombia), and Africa (Egypt, Ghana, Senegal, South Africa). Aker Solutions locations include Norway, UK, USA, and Australia. Available information regarding each companies' location, type of asset, position in market landscape, ownership and status, and criticality will be tabled in Appendix A under 'Company renewable market landscape'. Listed in Table 1 below, elaborates on the uncertainty and complexity of renewable production in different geographies, as linked to the discussion in chapter 2.2.1. The

in-text citation sources pertaining to Table 1 will be listed in Appendix A under ‘In-text citations for Table 1’, and any relevant abbreviations will be listed under ‘List of Abbreviations’.

Table 1 Market landscape concerns for the listed countries

Location	Regulatory environment	Financial environment	Technological and renewable development	Political climate
Norway	Strong regulatory support for renewables, active participation in EU energy policy. 90–95 % emissions reduction goal by 2050.	Favourable financing conditions with access to public and private funding.	Strong focus on various forms of renewable development. Extensive access to grid.	Stable political (socio-democratic) environment, supportive of clean energy policies. EU introduced the Green Deal Industrial Plan (2023) aimed at large-scale renewable expansion.
Sweden	Strong regulatory support for renewables. The country has committed to fossil free energy production by 2045.	Favourable financing conditions with access to public and private funding.	Favourable geographical conditions for renewable energy production accompanied by large-scale nuclear power development.	Stable social democracy with the highest share of renewable energy in the EU. 90% of the country's electricity is fossil free (43% from hydropower, 31% from nuclear, 16% from wind power).
UK: England Scotland	Strong regulatory support for renewables, active participation in EU energy policy. Net zero target is 2050.	Favourable financing conditions with access to public funding.	Strong focus on various forms of renewable development. Extensive access to the grid.	Stable political (democratic) environment, supportive of clean energy policies.
Ireland	Strong regulatory support for renewables, active participation in EU energy policy. Net zero target is 2050.	five-year strategy in place to increase R&D, making Ireland a global leader in innovation. Public, private, and international funding is available to further push the energy transition.	Ideal geographical location for offshore wind.	Stable parliamentary republic with strong climate change ambitions. Actively communicating and developing partnerships with energy organisations to support climate goals.
USA	General increase in incentives to move away from fossil fuels but	Availability of tax incentives, but policy instability can cause	High level of technological development and	Democratic, but divided political environment. Mixed

	there is divided regulatory support between states. Net zero target is 2050.	financing challenges. There is overall investment growth.	established renewables market with large wind development.	support for clean energy policies. Signed 2022 Inflation Reduction Act (IRA) as the largest climate change investment plan in US history.
Australia	Policies in place for achieving 43% emission reductions by 2030, 82% national renewable electricity target by 2030 and net zero by 2050.	Access to government funding and tax incentives, but private investment can be challenging. Commitment of $20 billion low-cost financing for upgrades to the electricity grid.	Recognition of extensive natural energy sources and opportunities. Large technological development in offshore wind, solar, hydrogen, and electrification.	Stable parliamentary democracy advocating for increase in renewable energy through various government agencies and consistent progress reporting.
South Korea	Renewable energy to account for 30-35% of generation by 2040. 2020 pledge of achieving carbon neutrality by 2050.	The country has a strong manufacturing base and can invest more into R&D as well as competence building for the renewables sector. This will allow South Korea to become a global renewables leader. Furthermore, the country has a variety of funding programs to support renewable expansion.	Strong focus on renewables, attractive market, world-leading supply chain, including yards and fabrication to industrialise floating wind.	Stable democratic republic with strong engagement with environmental organisations to pursue renewable energy. Ongoing cooperation with international governments and resources to expedite the energy transition.
Japan	Country has implemented robust policy measures aimed at expediting investments in clean energy. Carbon neutral goal by 2050, with 46% reduction in GHG by 2030.	Country has created a five-pillar framework to acquire investments from public and private partnerships, already allocating 20 trillion yen via government funding.	Pushing for zero emissions technologies such as biomass, hydrogen, ammonia, carbon capture, utilisation, and storage (CCUS), and wind power.	Japan is a stable constitutional monarchy. Strong renewable advocacy, taking proactive measures to reduce carbon emissions such as incentivising companies to reduce emissions through the GX league.
Vietnam	Net zero goal by 2050, with ambitious policy goals to promote transition.	International Partners Group (IPG) and Vietnamese leaders to support transition goals and enable JETP (Just Energy	Rapidly developing renewables market, strong hydropower, solar and	A stable socialist republic with a single party system governed by the Communist Party. Freedom of speech is

		Transition Partnership). Current non-bankable PPAs are a main risk factor for attracting investors.	both offshore and onshore wind resources.	restricted, and corruption is widespread. Main goals include economic growth, with consistent support to achieve net zero target.
Philippines	Strong renewables support, with a goal of 35% renewable energy share for total generation by 2030 and 50% by 2050. Currently no net zero emissions strategy update.	Increasing support for development via international partnerships and grants. Currently there are financial stability concerns affecting Philippines banks. A roadmap is in place to increase public/private, financing initiatives and development bank support.	Piloting green hydrogen and fuel cell systems for power provision. Strong potential for solar and wind power. Taking measures to strengthen the grid and electrify as well as explore the feasibility of nuclear energy.	Stable democratic environment with strong political desire to pursue renewables, although there are significant bureaucratic barriers constricting renewable development.
Chile	Strong regulatory support for renewables, ambitious carbon neutral goal by 2050. Implementing necessary policies and regulatory taxations to eliminate emissions.	Supportive green financial institutions (internally and externally). Chile is considered among the most attractive countries for investment in renewable energies.	2022 challenging market conditions due to grid capacity limitations. Strong potential for wind, geothermal energy, solar energy, and green hydrogen export.	Stable democracy supportive of clean energy policies. Newly written constitution (2022) concerning human rights issues. Country has a history of unrest with indigenous people, which could pose a threat to power projects.
Colombia	2030 aim to reduce emissions by 51%. Aim is to increase climate ambitions and forward technological, institutional, and territorial approaches to achieve carbon-neutrality by 2050.	Supportive internal financial regulations, including renewable energy auctions. Supportive external funding sources such as: UK International Climate Fund (USD 305 million), CIF (70 million) and USAID (USD 2 billion in 2023).	Hydropower is becoming less reliable due to climate change. Although, the country has rich renewable resources and strong potential for solar and wind power.	Unstable political climate with ongoing internal conflict, political unrest, and significant corruption. Challenging human rights situation, complex land issues rights, and extensive drug trafficking.

Egypt	Strong regulatory support for renewables, with 2035 aim of renewable energy contributing to 42% of power capacity. Currently no net zero emissions strategy update.	International financial support is important to assist in price management and decarbonisation. As of 2018, local financial institutions did not perceive renewables as low-risk investments, despite their cost-competitiveness.	Developing, with large potential for hydrogen, solar and wind market. Aims to expand grid connections across the Arab region and become an energy hub between Europe, Asia, and Africa.	Stable political environment (democratic republic), supportive of clean energy policies.
Ghana	Progressing regulatory support for renewables, with consistent efforts in place to increase renewables capacity and electricity access. 2022-2070 transition framework to net zero.	Limited access to long-term funding. Policies are in development to increase global funding through different international sources and public private partnerships.	Efforts in place to develop grid capacity and full access to electricity by 2030. Developing Renewable innovation to reduce CO_2 intensity through nuclear power, CCUS, and hydrogen fuel.	Stable democracy with efforts in place to improve renewable energy capacity. Although policy instability and uncertainty does pose a threat to development.
Senegal	Currently no net zero target. Undergoing significant energy reform to implement renewable projects, combat high prices and unequal supply. Initiatives include carbon pricing and subsidies for low-income households and improving university renewable programs. There remain strategic gaps in policy, requiring further improvement.	Reform processes are outpacing the available human and financial resources. There are limited local bank and financing options. Although, there is increasing international development bank support.	Rich natural resources. Stable and well-developed grid. Strong potential for solar and wind energy. Hydrogen and CCUS under development.	Stable democratic government, motivated to participate in the energy transition. Although, the governmental strategy is non-transparent, thus increasing international stakeholder concern.
South Africa	Net zero target by 2050. Strong regulatory support from the Clean Energy Transition Programme, EU, and partners of the Just Energy Transition Investment Plan, with aims to increase renewables capacity.	Access to public funding and private investments with supportive financial institutions, including the IPG and revenue streams from mineral extraction, to support the transition.	Strong potential to reduce GHG emissions, focus on: CCUS and natural gas transportation. Renewables focus: Solar Photovoltaic and hydropower. Currently very coal dependent.	Political uncertainty is high in terms of instability and corruption, which can have an adverse impact on renewable support schemes.

2.3 Closing remarks on risk type correlation and company landscape

It is the author's aim that by including components of the IRGC Risk Governance Framework in this thesis, recommendations can be formulated to improve not only risk assessments but greater risk awareness and management within the renewable energy sector. It is prudent to note that when assessing the types of risk problems pertaining to the renewable energy market, one must keep in mind the interdependency of the world market, where the risks placed on the companies depend greatly on the bureaucratic processes within the specific region. It is in the same vein beneficial to remember that the Risk Governance Framework, from which these principles derive, work optimally in liberal democratic societies, wherein not all renewable production is at present or planning to be. Ultimately, by concluding that renewable production is an uncertain and complex risk problem, the choice of management option can then be analysed by means of the cautionary/precautionary and risk-informed approaches, which will be discussed in chapter 4. These approaches are considered due in-part to the newness of renewable technologies and assets within the energy sector, when compared to that of oil and gas. Additionally, these approaches will assist in gaining a better understanding of the above ground physical risks associated with the geographical location and the market landscape of renewable production, in which the companies operate. Going forward, chapter 3 will compare the security approaches, security reporting, and security risk assessment methods between the analysed companies.

Chapter 3
Security comparisons

Due to competitive innovation associated with the rapidly evolving renewable energy sector and its increasing attractiveness as a target to threat actors, amplifying security awareness is advisable. This will help secure the energy transition and minimise detrimental social, environmental and company impacts. The security information in this chapter assists in generating a security picture concerning both the renewable and oil and gas sectors, thus facilitating a comparative analysis on how they differ. Moreover, this analysis helps identify whether current security risk management practices are being optimised on renewable production. By creating an overview of relevant threats and the differences in security practices, renewables companies can better analyse and effectively address potential gaps. This chapter serves as a starting point for increasing risk awareness and provides a platform to assess appropriate solutions and tools suited to company margins and needs, which will be discussed in greater detail in chapter 4.

In this chapter, relevant security risk management practices of the analysed oil and gas versus renewables companies will be examined. Comparative data will include the following:

1. Current security reporting practices and Security Risk Assessment (SRA) methods between the analysed companies (Chapter 3.1).

2. Comparison of the following security categories identified by each company: main threat types, associated and relevant impacts, and threat actor capability and intent categories (Chapter 3.2, 3.3, 3.4).

Information regarding chapter 3.1.1 was collected through recent company annual and sustainability reports. Information concerning the rest of the chapter was collected by interviews from heads of security within each company, including the heads of security at Aker ASA, who provide support to Aker Horizons across their renewable portfolio on security risk management.

Categories in chapters 3.2, 3.3, and 3.4 are primarily informed by Aker ASA, unless otherwise stated.

3.1 Company risk practices and SRA processes

This chapter analyses the companies' use of risk concepts, principles, methods, and approaches when reporting security practices and conducting an SRA. Furthermore, the comparisons will focus on the cyber and physical (malevolent) security risks directly targeted at contracted employees, assets, and clients. Comparative information and risks not analysed include but are not limited to the following: reporting policies, audit schemes, risks affiliated with human rights violations and slavery in the supply chain, climate (weather) related risks, legal risks, associated financial risks, and in-depth market risks. Contextual mention of the above may be necessary, but it is not the focus of this chapter. Relevant sources and company information including descriptions of abbreviations and elements pertaining to chapter 3.1.1, specifically Table 5, will be listed in Appendix B under 'Security practices between the companies.'

3.1.1 Comparing reported security practices between the companies

Table 2 Company security focus areas

Company	Aker BP	Aker Solutions	Aker Horizons (Mainstream RP)
Security focus areas	Cyber (Top priority) Personnel (insider) Physical (outsider)	IT (cyber security) /Data privacy Personnel (insider) Physical (access control/ barriers) Travel	IT security Personnel security Physical risks: Weather/climate ESG (Environmental, Social, Governance)

Table 3 Company security standards & frameworks

Company	Aker BP	Aker Solutions	Aker Horizons (Mainstream RP)
Security standards & frameworks	ISO 31000 (ERM) Voluntary Principles on Security and Human Rights	ISO 31000 ISO 27001 (Information Security Management system) NIST (National Institute of Standards and Technology) SP 800-53 framework (Data privacy/IT risks) ISO 22301 (emergency and crisis management/ business continuity) Committee of Sponsoring Organizations of Treadwell Commission (COSO) framework Project Management Institute	ISO 27001

Table 4 Company security risk management tools and practices

Company	Aker BP	Aker Solutions	Aker Horizons (Mainstream RP)
Security risk management tools & practices	Quarterly HSSE and cyber security reporting. This is coupled by regular review with audit management on major identified risks. Activities are completed via the ERM process. Risk metrics: Calculated risks and opportunities based on probability and associated consequences.	Risk monitoring and mitigation is reviewed quarterly by the audit committee and includes uncertainty estimates and climate related risks. This is coupled by annual ERM review. Risk metrics: All risks are given a score based on probability and impact.	Quarterly ERM assessments and annual assessments of entire risk matrix. Risks and measures are reviewed by the audit committee. ERM risk identification templates, sessions, and assigned risk treatment plans.

	Three Lines of Assurance based risk processes and tools for internal auditing. Any residual risk is quantified and verified to be within Aker BP's risk acceptance criteria. Monitoring and mitigation: Regular intelligence, value, and threat assessments. Continually updated record of security controls/barriers and weaknesses. Continually updated record of threat actors. Integrity due diligence (IDD) checks on suppliers and business partners. Employees required to take annual cyber security and barrier management courses. Regular preparedness and response training for critical security incidents. Security personnel undergo background checks.	Specific tools for each risk category on how to assess, respond, and report risk. Tools used include internal controls, scenario planning/analysis and sensitivity analysis. To mitigate risk to an acceptable level, risk owners implement controls such as new or improved procedures. Continually monitored threat landscape to identify malicious activities. IDD assessments and country risk assessments are conducted to assess corruption, crimes, terror financing, and other material risks. Continual improvement to secure emails. Mandated annual phishing email/cyber security exercises to increase employee awareness to cyber-crime. Emergency preparedness structure based on a three-tiered approach. Regular emergency response exercises are conducted. Standardised risk management process across all projects.	Structured threat, climate risk, incident, and impact monitoring, reporting, and response procedures. Regular IT vulnerability assessments and testing. Regular Scenario analysis on climate risks. IDD screening. Regular IT (cyber) security training and emergency preparedness training.

Table 5 Company security-focused business areas & systems

Company	Aker BP	Aker Solutions	Aker Horizons (Mainstream RP)
Security focused business areas & systems	ERM (Enterprise risk management) HSSE system and SEAC (top priority) TCFD (Task Force on Climate-related Financial Disclosures) EPR (Emergency Preparedness and Response) SMS (Security Management System) BMF (Barrier Management Framework) Three Lines of Assurance/ BMS (Business Management system)	ERM & TCFD HSSE system Emergency Preparedness and Response Framework (CERT: Corporate Emergency Response Team)	ERM HSSE system TCFD GDS (Global Development Standard) PPM (Project Portfolio Management)

Table 6 Company key security developments

Company	Aker BP	Aker Solutions	Aker Horizons (Mainstream RP)
Key security developments/ measures	Threat Intelligence capacity program implemented to reduce uncertainty.	Cyber insurance purchased (2022/2023). Implemented central logging system with 24/7 security operations centre.	Stress testing for climate risks. Goal: standardise risk management across company. Develop system to track critical climate risks and policy developments. Plans to introduce more detailed quantitative risk assessments for climate risks.

3.1.2 Comparing SRA methods between the companies

Aker BP

Approach to security risk management:

The company claims to have a good view of their threat landscape and how attractive they are to threat actors. Relevant data concerning various types of threat actors and their capability, intention and attractiveness to the company is acquired in collaboration with relevant subscription services and companies, as well as through the use of threat assessments generated by government resources. This information, which defines criminal actors and enduring threat scenarios for onshore and offshore assets, is placed into a threat library and allows the company to categorise them within low, medium, and high-risk zones. Moreover, Aker BP's proactive approach to security is exemplified by its management of security incidents related to drone sightings. To address this issue of potential espionage threat, the company is actively developing radar systems capable of detecting and identifying drones in both aerial and subsea environments. Additionally, the company has established a collaboration with Equinor to implement suitable risk reduction measures.

The company does, however, acknowledge a need to create a more centralised overview of security risks by implementing a more systematic, dynamic, and practical approach to holistic security management, which can be used by all business units. The goal is to improve communication and make the management of security risk more structured, predictable, and efficient. To actualise these goals, Aker BP intends to veer away from current "paper-based practices", which is deemed as inefficient, and move towards a more dynamic and non-linear approach, which does not require continual manual input and updating. Ultimately, the company has identified "root causes" associated with their risk management concerns and has solutions and goals in place to address them as part of their risk framework for security.

The SRA process:

The SRA processes for managing physical risk and cyber risk are the same, although international security standards vary and are implemented accordingly for each type of risk. Specifically, ISO 31000 is implemented, but cyber security also uses security frameworks such

as CIS (Center for Internet Security) and NIST, neither of which are stated in reports, and the newly developed Omny Security software. In short, the current SRA process consists of 1) establishing context (asset assessment and threat assessment); 2) risk identification (select risk events); 3) risk analysis (threat analysis and consequence analysis); and 4) risk evaluation (establishing risk picture). Each step within the process is coupled by communication and consultation, alongside monitoring, review, and updates.

Traditionally, SRAs have been conducted on assets according to their respective reports, and dimensioning risk outcomes were formulated in connection with potential scenarios. In the case of offshore reports, 14 dimensioning scenarios were typically devised by a single employee. However, this methodology carried the inherent risk of cognitive biases influencing the assessment outcomes. Moreover, this traditional way of conducting SRAs yielded static and one-dimensional assessments, which fails to capture the current risk landscape, the dynamic threat environment, or the chain reaction of possible events. Going forward, a more dynamic and easier to navigate approach will be piloted. This will assist asset owners in comprehensively managing their security risks by having a complete overview of barriers, relevant threat actors, relevant attack scenarios, and relevant measures to reduce risk to acceptable levels.

Use of risk management tools:
The company, via Aker ASA and in collaboration with Telenor and Cognite have established a new company by the name of Omny Security, which has developed a cyber and OT (operational technology) risk management tool. The Omny software will work to calculate risks in real time, thus securing industrial operators and infrastructure based on assessments of different sequences, parameters, and functions in a given process. The software will have an overview of entities, assets, controls, threats, and scenarios. Therefore, when mapping the tool to different assets, the algorithm will use enhanced predictive measurements through scenario analysis, to assess context changes, and better measure uncertainty, vulnerabilities, and confidence. Ultimately, the dynamic nature of the tool's software will allow for operations and security teams to gain greater and more accurate visibility associated with industrial security threats. Moreover, the risk buffer will be able to measure current risk, risk acceptance, and daily value creation in USD.

In consideration:

Information pertaining to employing the oil and gas approach of security to renewables is not relevant for discussion in this section as Aker BP is a pure play upstream oil and gas company.

Aker Solutions

Approach to security risk management:

The company claims to have a satisfactory view of security from the top through its support from Aker ASA but acknowledges a need to improve visibility from the operational level to what is happening on the ground. Among the considerations for employing a security measure, the following are key considerations the company takes when going through the decision-making process: evaluation and review of risk categories and their Jotform outcome, the profitability of the project, and the criticality of the customer relationship and their risk appetite.

The SRA process:

The company uses frameworks such as ISO 31000, Project Management Institute, ISO 27001, and NIST SP 800-53 when conducting their SRAs. Moreover, the company requires asset owners to conduct maturity assessments, in which the owner is required to answer relevant questions regarding required security policy documentation, including when an SRA was previously conducted, by whom, and if there is a nominated third-party provider. The procedure then uses Jotform, which employs a click form based system to assess all risk categories. This system uses a consequence matrix from 1 to 5, including several identified scenarios and questions tailored to suit the risk categories. Questions can take the form of assessing the number of muggings, violent break-ins, and employee violence, among others. If multiple scenarios are answered confirming a scenario, the company assesses the highest rated risk. If for example an active shooter is assessed and confirmed to be the highest rated risk, an assessment of likelihood and consequence of this scenario will be carried out to give a risk rating for violent crime. Other questions may relate to barrier systems concerning but not limited to perimeter fencing, CCTV, guards, and shift schedules. In terms of cyber risk, the security department is a stakeholder, in which the IT department primarily manages the risk of cyber-crime. It is understood within the company that the starting point of a cyber breach stems from a physical breach. Within Jotform, questions pertaining to employee exposure to ransomware and phishing emails may be asked. An

affirmative response to any of these questions triggers follow-up conversations with the IT department.

Use of risk management tools:
Risk matrices are used with pre-defined categories from 1 to 5, where scoring is calculated by means of consequences and probabilities. Otherwise, there is no implementation of academic risk tools internally when conducting SRAs. The security culture within the company emphasises output and framing a meaningful discussion on risk management, rather than performing perfectly standardised SRAs.

Employing the oil and gas security approach to renewables:
Aker Solutions as an engineering, procurement, and construction company for both the renewables and oil and gas industry is not an operating company and therefore employs the same security approach to all types of assets. Although, the way in which the company segments are set up, including emergency response combined with the differences in experience and competence, means that there is a difference in the way events are managed. While the management or handling of events vary based on the desired or expected outcome, in principle they are managed the same way. As a provider of solutions, the company experiences risk one tier below the operating company, with the main risk to construction of any asset being petty crime.

Aker Horizons (Mainstream RP)
Approach to security risk management:
The company claims to have a top-down approach to security, meaning the company does not have the same degree of ground visibility from the operational level. Furthermore, the company claims to have a reactive approach to security at the local level. Where and when necessary, security measures are repaired, or new measures are implemented to strengthen barriers and controls following security incidents.

The SRA process:
The SRA processes for managing physical risks and cyber risks are the same, although both vulnerabilities and international security standards vary and are implemented accordingly for each type of risk. However, the ISO 27001 framework is the only security focused framework listed in the annual sustainability report by both Aker Horizons and Mainstream RP.

Use of risk management tools:
There has been no implementation of academic risk tools internally, however Aker Horizons uses outside vendors, which cover many forms of risk and are updated on a regular basis.
The company also employs Omny Security to assess cyber risks.

Employing the oil and gas security approach to renewables:
The cost of security for oil and gas assets are understood as substantial but justified. Employing this approach to renewables is considered too costly. When evaluating offshore assets, the company acknowledges their remoteness from threat actors, whereas onshore assets are primarily at risk of losing critical materials to crime. Barriers shall be in place to minimise impact to operations.

3.2 Comparing threat type categories

The Society for Risk Analysis defines threat within a security risk setting as a risk source with "a stated or inferred intention to initiate an attack with the intention to inflict harm, fear, pain or misery" (Aven et al., 2018, p. 7). Smith and Brooks (2013) state that many risk management standards such as ISO 31000, which both Aker BP and Aker Solutions use, do not take threat into enough consideration, it is therefore important that threat is clearly conveyed within a company's security risk management process (Smith & Brooks, 2013).

All threat categories presented in Table 7 are based on Aker ASA and individual company interviews and their recognition of threat types, which have the ability and possible intention to inflict harm. "X" indicates acknowledgement of category.

Table 7 Comparing identified threats between the companies

Company	Aker BP	Aker Horizons (Mainstream RP)	Aker Solutions
Cyber and OT	x	x	x
Sabotage	x	x	x
Armed conflict		x	
Civil unrest		x	
Crime	x	x	x
Espionage	x	x	x
Terrorism	x	x	x
Subversion	x	x	x
Insider threat	x	x	x
Activism	x		x

3.2.1 Threat category information

Relevant definitions and or notes on each threat category pertain to the individual companies, and are listed as follows:

Cyber and operational technology (OT)

Cyber and OT refers to malicious actors attempting to manipulate or corrupt the organisation's IT system, processes, or personnel to achieve their own goals. For the analysed companies, cyber security risk levels are evaluated as high and top priority. Consequences from actual or perceived breaches of network security can cause significant harm to business performance and reputation. Risks include significant loss of intellectual property, financial loss, information data loss, data privacy infringement and system irregularities and downtime (Aker BP ASA, 2023a); (Aker Solutions ASA, 2023a). The most common vector of cyber-crime derives from phishing emails, which can result in unauthorised access, malicious code, or denial of service attacks. The current concern among all companies are the geopolitical disruptions caused by the ongoing war against Ukraine, leading to increased risk of cyber security breaches. Mitigating actions include strong security controls and security competence building among employees.

Sabotage

Sabotage refers to the deliberate and malicious intent to cause harm and disrupt operations of an organisation, business, government, or individual. Sabotage can be motivated by many reasons, although Aker ASA acknowledges that, due to geopolitical instability and Russia's continued efforts to destabilise the West, there remains the possibility of pipelines, as well as LNG (liquefied natural gas) terminals, being attractive targets for Russian sabotage.

Armed conflict

Armed conflict broadly refers to the presence of violent conflict between two or more groups seeking personal gain, such as maintaining or gaining territorial occupation. Aker ASA, Aker BP, and Aker Solutions do not consider armed conflict to be a threat category, although, Aker Horizons (Mainstream RP) perceives armed conflict to be a relevant threat category in terms of their exposure to conflict between indigenous groups and disputed land areas in Chile and Colombia.

Civil unrest

Civil unrest is exacerbated in countries with institutional and societal weaknesses, such as political violence, economic inequality, environmental deterioration, and climate change (Dalby, 2017); (Boin et al., 2020). Notably, political violence increased globally during the Covid-19 pandemic, according to Aker ASA. Moreover, the unstable political climate in Chile and Colombia, coupled with ongoing internal conflicts, and aggravated by Colombia's drug trafficking, poses a potential threat to operations. Aker Solutions and Aker BP do not include civil unrest in their threat assessments.

Crime

Aker ASA and Aker Horizons (Mainstream RP) define crime as opportunistic and organised, while Aker Solutions defines crime as both non-violent and violent. The companies are exposed to armed robberies as well as cyber-crime. Additionally, Aker BP acknowledges that their advanced digital profile increases attractiveness to crime.

Espionage

Espionage is categorised within the information security domain. Aker Solutions defines information security threats as the physical gathering of information and intellectual property via insider threat. Aker Horizons (Mainstream RP) defines espionage as commercial espionage because of the fast pace in which the market is growing. The companies take the position that where there are technological developments, there will be nation state and criminal actors motivated to conduct industrial espionage. There is difficulty in determining if espionage has or is happening, although Aker Horizons takes the position of assuming that both apply, thus taking a proactive approach to management. Convincing stakeholders to spend money on mitigating measures without seeing the threat is challenging, although due to target attractiveness based on the high value of the company, the modern technology used, and strong employee competence, implementing mitigation measures is adequately supported. A proactive approach is also adopted by Aker BP to the possibility of espionage, which is evident in their mitigation measures concerning the presence of aerial and sub-sea drones.

Terrorism

The types of terrorism which can impact an organisation includes but is not limited to "eco-terrorism (against private organizations), cyber-terrorism (hacking, identity theft, and fraud), and corporate terrorism (ransom, public reputation)" (Smith & Brooks, 2013, p. 245). Aker ASA assesses terrorism as being incidental but not directly targeted at any Aker company, although this could change in the future.

Subversion

Aker ASA and Aker Horizons (Mainstream RP) view subversion as the individual or group (within or outside of an organisation) as having the intent to weaken the systems or values of an organisation. It is classified as anything that is connected to influence campaigns to change strategy or the narrative within a company. Within the companies, subversion falls under the categories of cyber security, insider threats, and social engineering. Aker Solutions does not consider subversion as a distinct threat category, but it is understood as a risk/scenario within the personnel security risk management process.

Insider threat

Aker ASA, on behalf of its portfolio companies, defines insider threat as “the threat posed by unauthorised access, use or disclosure of privileged information, techniques, technology, assets or premises by an individual with legitimate or indirect access, which may cause harm” (Aker ASA, 2022, p. 17). The company acknowledges insider threat due to the target attractiveness of the Aker companies. Furthermore, the company assesses insider threats as both unintentional and malicious. The unintentional insider can be “trusted employees or contractors that inadvertently expose, or make vulnerable to loss or exploitation, privileged information, techniques, technology, assets, or premises. (The trigger of this threat is the) lack of security awareness and failure to follow security protocols. (The malicious insider can be either self-motivated or recruited by a third party and are) trusted employees and contractors who deliberately and wilfully breach their duty to maintain the security of privileged information, techniques, technology, assets, or premises. The motivation is often financial gain, or to cause harm, loss or damage” (Aker ASA, 2022, p. 17).

Activism

Aker ASA does not include activism as a direct threat category due to the majority of activism being conducted within the legal limits of freedom of speech. The company does not include activism in their identification of extremists due to the possibility of the word being misconstrued. Aker Solutions and Aker BP do, however, list activism as a threat category and acknowledge the activist threat in Norway to be increasing, both in terms of violence and information security breaches. With Aker Solutions’ connection to the oil and gas industry, activism towards a key partner, such as Equinor, could impact Aker Solutions, as Equinor oil rigs are in Aker Solutions' shipyards. The biggest risk concern of an activist led event is the safety and security of the demonstrators themselves. The company claims that it would be reputationally, commercially (customer relations) and strategically (market value) catastrophic if a demonstrator were to be injured or killed at an event on Aker Solutions compounds. The consequence of injury to a demonstrator could lead to an increased desire for customers to no longer wish to be associated with the company if this risk was not managed appropriately. Cases of activism in the future could be linked to NIMBY (not in my backyard) protests, ecosystem disruptions, and fishermen conflicts.

3.3 Comparing impact categories

The Society for Risk Analysis defines impact as “the effects that the consequences have on specified values (such as human life and health, environment and economic assets)” (Aven et al., 2018, p. 6).

Malicious attacks on the energy sector can have damaging financial and reputational impacts to a business. Security breaches can negatively impact personnel and have severe effects on the environment as well as the social landscape to which the energy is provided.

All impact categories presented in Table 8 are based on Aker ASA and individual company interviews and their recognition of how their company landscapes can be negatively impacted. “X” indicates acknowledgement of category.

Table 8 Comparing identified impacts between the companies

Company	Aker BP	Aker Horizons (Mainstream RP)	Aker Solutions
Operation (financial and reputational)	x	x	x
Personnel	x	x	x
Environment/Climate	x	x	x
Social	x	x	x
Strategic (values)			x
Legal and compliance			x

3.3.1 Impact category information

Relevant definitions and or notes on each impact category pertain to the individual companies, and are listed as follows:

Operational (financial and reputational)

Impacts include downtime for construction, revenue loss and induced costs. The operational impact for Aker Solutions includes financial and commercial impacts, which is defined as the long-term impact to relationships with long term clients. For Aker Solutions, reputation is considered its own impact category. For Aker BP, both financial and reputational categories are separated.

Personnel

Personnel security for Aker Solutions is defined within health and safety and includes people and PMO (Project Management Office) processes. Aker Horizons analyses and generates risk data on specific locations of operation, particularly concerning travelling employees. Travel security is a mature focus across the Aker chain, and uses a shared system called Aker Security Services, which supplies briefings and pre-trip advisories to any travelling employee prior to departure. Furthermore, the company can provide cellular tracking devices to employees departing to high-risk locations, which are monitored 24/7 by a global security operations centre (GSOC). GSOC also uses the Everbridge (International SOS) system. Furthermore, Aker ASA provides both six month and yearly updates of overarching threats to the Aker group concerning relevant geopolitical threats.

Environment/Climate

Attacking renewable infrastructure can result in a reduced energy output, which could lead to a reliance on traditional fossil fuels, whereas attacking an oil rig or pipeline could contaminate bodies of water and harm aquatic life. Furthermore, the act of sabotage could emit unintended and immense volumes of GHG into the air, as was the result following the sabotage of the 2022 Nord Stream pipelines in the Baltic Sea.

Social

Social consequences associated with a security breach can include the disruption of power supply within a country or jurisdiction, which could result in a reduction of power to hospitals, schools, and industry. Within the Aker group, social impact is broadly defined as corporate social responsibility and good governance, guided by ESG principles. This includes but is not

limited to the impact on local communities, supply chain, and personnel. The overarching goal across the Aker portfolio is to mitigate any adverse impacts from all operations.

Strategic (values)

Aker Solutions defines strategic value impacts as significant loss of market value. This Impact category is only used by Aker Solutions.

Legal and compliance

Security threats can impact the company's ability to meet contractual deliverables with suppliers and customers, which can lead to possible legal action and reputational damage. This impact category is only used by Aker Solutions.

3.4 Comparing threat actor capability and intent categories

Although the Society for Risk Analysis does not specifically define threat actors, they do define exposure, which is the condition of "being subject to a risk source/agent" (Aven et al., 2018, p. 6). Risk source/agent is defined as the "element (action, sub-activity, component, system, event, etc.) which alone or in combination with other elements has the potential to give rise to some specified consequences (typically undesirable consequences)" (Aven et al., 2018, p. 7).

In a security risk management setting, Smith and Brooks (2013) define threat as the sum of intent and capability, where it is "the threat agent that causes a threat to happen" (Smith & Brooks, 2013, p. 64). Intent can be further understood as the motivation to cause damage.

All threat actor capability and intent categories presented in Table 9 are based on Aker ASA and individual company interviews and their recognition of malicious actors who may have capability and intent to negatively impact the company. "X" indicates acknowledgement of category.

Table 9 Comparing identified threat actors between the companies

Company	Aker BP	Aker Horizons (Mainstream RP)	Aker Solutions
State actors	x	x	x*
Proxy actors		x	x*
Criminals	x	x	x*
Extremists	x	x	x*
Activists	x		x*

*Aker Solutions has not formally categorised threat actors, although, as per the company interview, these categories are applicable and acknowledged.

Figure 1 represents the relative weight assigned to each threat actor category based on their capabilities and prevalence, as determined by Aker ASA.

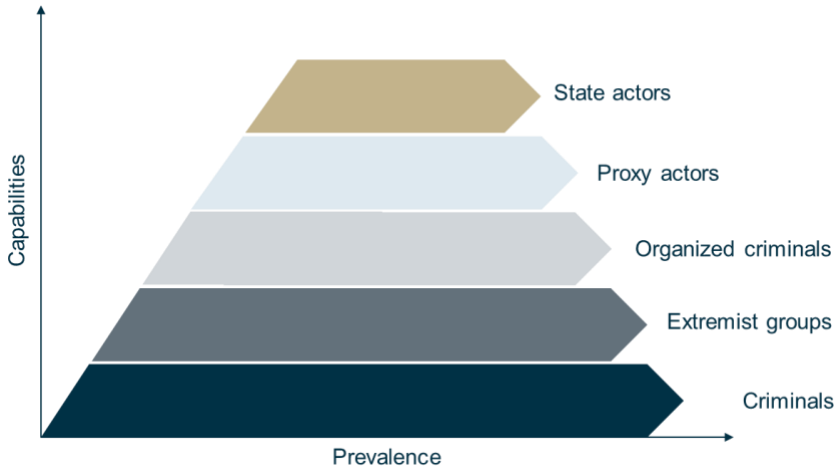

Figure 1 Threat actor capability & prevalence scale for Aker ASA (Aker ASA, 2022)

3.4.1 Threat actor category information

Relevant definitions and or notes on each threat actor capability and intent categories pertain to the individual companies, and are listed as follows:

State actors

In 2022 Aker ASA acknowledged an increasing concern of advancing collaborations between states and cybercriminals, with growing commercial markets for the sales of cyber weapons. The company recognises a need to proactively defend their networks against the increase of cyber weapons, which can severely impact organisations and the societies who benefit from their energy supply. Aker BP acknowledges a 25 percent likelihood that state actors will be a serious threat to the company within the next year. Malicious aims include influencing commercial affairs, stealing technology and R&D, and disrupting infrastructure. State actor objectives could be to improve the competitiveness of domestic companies via use of any of the relevant threat categories. Stealing technology could be motivated by its capability to produce significant commercial or military competitive advantages. A possible motivation for disrupting infrastructure may also be to undermine energy supply of Norwegian and NATO forces in a crisis, which demonstrates resolve and capability to Norwegian authorities over a political issue, and tests capabilities. Computer and network operations are predicted as likely vectors, and employees as likely targets.

Proxy actors

Proxy actors operate within the cyber and physical realm and act on behalf of another in a network or system to hide the identity of the original actor and conceal intent. This makes it challenging to detect and mitigate security threats. Malicious actors' intentions may be to launch attacks, bypass security measures or evade detection. Aker ASA acknowledges that in the face of war, proxy conflicts can be triggered or evolve without notice. Aker BP does not include proxy actors as a direct category.

Criminals

Aker ASA identifies both criminals and organised criminals. Aker BP acknowledges a 13 percent likelihood that criminal actors will be a serious threat to the company within the next year. Increased digitalisation induces further vulnerabilities due to its attractiveness, and company network operations are predicted to be likely targets. Organised criminals may also have the intent of committing petty theft (stealing valuables) and or using facilities for their own malicious intent.

Extremists

Extremism can arise from intensified animosity from one nation to another. Aker ASA acknowledges the motivation for Russia to intensify its offensive against Western political systems via funding extremism and influence campaigns. Aker ASA further identifies the possibility of Russia diverting NATO's attention from Ukraine by instigating disturbances in the Balkans.

Activists

Activism is an increasing concern to the oil and gas sector and affiliated industries. According to Aker BP, vectors of activism led events are predicted to include infiltrating compounds, PR-campaigning, lobbying, and computer network operations. As stated, Aker ASA does not include activism as a direct category.

Chapter 4
Discussions

This chapter is divided into three main sections:

1. Chapter 4.1 expands on the analysis in chapter 2 and discusses appropriate risk management strategies and tools suited to address the identified uncertain and complex risks associated with market dynamics.

2. Chapter 4.2 builds off both chapter 2 and 3 by analysing risk tolerability associated with market and security risks of both the oil and gas and renewables focused companies.

3. Chapter 4.3 builds off the company analysis in chapter 3 and discusses suggested security practice improvements, viable for application towards the analysed renewables companies.

Information pertaining to chapters 4.2 and 4.3 has been collected through interviews with heads of security within each company, including the heads of security at Aker ASA, who provide support to Aker Horizons across their renewable portfolio on security risk management.

4.1 Appropriate risk management tools (for uncertain & complex risk)

The three risk-based strategies in risk management

Within risk management there are three classes of risk-based strategies/approaches used to manage risk. These are comprised of the risk-informed, cautionary/precautionary (resilience oriented), and discursive strategies. In brief, the risk-informed strategy treats risk through avoidance, reduction, and transfer of risk through risk assessments and is useful towards all risk problems with small, moderate, and large uncertainties. The cautionary/precautionary strategy manages risk and uncertainty through robust and resilient means such as increasing knowledge, containment, continual monitoring, and improving barriers through redundancy, maintenance,

and testing (Renn, 2017, p. 203). This strategy is useful towards complex risk problems experiencing moderate and large uncertainty. Finally, the discursive strategy is aimed towards ambiguous risk issues, in which cohesive, transparent, and homogenous dialogue between stakeholders is necessary, although at times challenging due to differences in values. This strategy does not refer directly to the degree of uncertainty, but to efforts surrounding communication and consensus on risk concerns. When referring to ambiguity, the weight given to risk issues discussed in this thesis pertain to the different concerns each individual company recognises according to their security department. Ambiguity regarding internal processes within the analysed companies goes beyond the scope of this thesis and focus is therefore directed at the risk-informed and cautionary/precautionary strategies for managing risk.

Degrees of uncertainty and the appropriate risk-based approach

When determining which risk-based approach was appropriate for this thesis, an assessment on the degree of uncertainty towards the risk problem was considered in reference to the IRGC Risk Governance Framework (2005) via Renn (2017) and Aven (2014). Chapter 2.1 highlighted that simple risk problems are those, in which the occurrence of an event and associated consequences can be predicted quite accurately. A simple example can take the form of traffic accidents, where there is a plethora of available data on accidents and risk exposure. These consequences contain minute uncertainties and are coupled by strong knowledge, allowing for the use of risk-informed strategies through probabilistic methods, statistical analysis, and risk analyses based on frequencies; refer to chapter 2.1. This is not the case concerning renewable production, climate change, and market factors in which the risks are much more uncertain and complex. A risk problem, which is complex, deals with the predictability of how individual components within a system interact as a whole. When addressing risks correlated with renewable production, chapter 2 concludes that the addressed risks are largely complex in terms of the individual components and their interactions within the market system. Furthermore, uncertainty connected to market dynamics, which also includes geopolitical instability and exposure to malicious threat actors, highlights the vulnerabilities associated with renewable energy security. Chapter 3.2 further elaborates on the security threats faced by the companies, with significant risks pertaining to cyber security and espionage, among others, and the consequential (and uncertain) occurrence of these events taking place. With this understanding of the diverse threat landscape, renewable

operations ultimately face both moderate to large uncertainties regarding market risks and security risks.

Within a complex system, there will always be a degree of uncertainty associated with the performance of the system due to the historical context in which data has traditionally been acquired, and tested against prior vulnerabilities (Aven & Renn, 2020). Although uncertainties will remain present, the most suitable approach for managing them will be through robust and resilient methods, which are dually linked to cautionary strategies. Having established that complex risk problems are a special case of uncertain risk problems, using a conjunction of multiple risk management strategies, including the risk-informed strategy, is ideal (Renn, 2017). Combining risk management strategies when deciding upon appropriate risk measures will further address the possibility of surprising events and black swans (Aven, 2014). Listed in Table 10 is an overview of management strategies for risks facing moderate to large uncertainties in accordance with the risk-informed and cautionary/precautionary-based management strategies.

Table 10 Management strategies for uncertain risk (Based on Aven 2014, p. 164)

Risk category	**Management Strategy**	**Appropriate instrument**	**Risk Tools**
Moderate uncertainties	Risk-informed	• Risk assessments • Broad risk characterisations • Cost-benefit analyses	• Containment • ALARP • BACT (best available control technology) • Etc.
	Robustness focused (risk absorbing system)	Improve buffer capacity and performance of hazard/threat risk targets via: • High performance standards of barrier systems • Additional safety factors • Redundant and diverse safety factors and devices • Improving coping capacity	
Large uncertainties	Risk-informed and caution/ precaution-based	• Risk assessments • Broad risk characterisations • Highlighting uncertainties and features such as persistence, ubiquity, etc.	• Containment • ALARP • BACT • Etc.

	Robustness and resilience focused (risk absorbing system)	Improving capability to cope with surprises via: • Diversity of means to accomplish desired benefits • Avoiding high vulnerabilities • Allowing for flexible responses • Preparedness for adaptation	

Going forward: suggested implementation of tools and measures

Upon consideration of the appropriate strategies for the context of uncertain and complex risks, the author acknowledges the importance of generating knowledge to support assessments. This has been achieved in this thesis thus far via risk-based comparisons, which were broadly carried out in both the market landscape analysis in chapter 2.2.2 and the company security practice comparisons in chapter 3. Going forward, the suggested approaches for application towards the renewables industry will take knowledge generation into account, to better assess the issue of uncertainty. Though there is an abundance of methods, strategies, and tools designed to manage uncertain and complex risk problems**,** this thesis highlights two methods that are particularly relevant when assessing appropriate security measures for renewable production. These methods include the ALARP (as low as reasonably practicable) tool and the 'systems approach' to decision-making. Chapter 4.1.1 will first analyse the cautionary and precautionary principle as a preamble to the ALARP tool, which has been chosen due to the lack of available and consistent data concerning renewable production and associated challenges when compared to that of oil and gas production. Chapter 4.1.2 goes on to acknowledge the implementation of the systems approach in accordance with the risk-informed management strategy, to improve the implementation and understanding of the interactions between risk measures.

4.1.1 Cautionary/precautionary based management strategies

Understanding the cautionary and precautionary principle

The cautionary principle implies that caution shall be the ruling principle over risky activities and its possible severe and or irreversible impacts in the face of 'understood' uncertainty, even if the measures (or in extreme cases, ban of the activity) are not cost-effective (Aven, 2014). The cautionary principle is not so much about 'scientific' uncertainties associated with unknown

cause-and-effect relationships. In this case, uncertainties related to an activity or event are understood, do exist, and could still occur, even if it is calculated with a low probability that the event will happen, for example, a fire. For instance, the cautionary principle can be implemented by installing access control systems and surveillance cameras to mitigate the negative consequences of potential security threats linked to unauthorised access.

The precautionary principle, in contrast, can be viewed as a specific application or special case of the more general cautionary principle (Aven, 2014). In this case, precaution shall be the ruling principle if there is presence of multiple high 'scientific' uncertainties as well as the possibility of severe impacts, where there is no conclusive evidence on the cause-and-effect relationship. This suggests that the full extent of the risk(s) is still uncertain (Renn, 2017) and precautionary measures should be taken, or the activity should not be carried out. For instance, organisations may implement robust firewalls, intrusion detection systems, and encryption protocols to safeguard sensitive data from unauthorised access and cyberattacks. By adopting the precautionary principle, organisations can anticipate and address potential vulnerabilities before they manifest into significant security breaches.

Scientific uncertainty exists to varying degrees within risk-informed decisions; therefore, value judgements will determine whether to take precautionary measures. The use of extended risk assessments, risk instruments, uncertainty characterisations, and risk-to-risk comparisons can aid in informing judgements of a risk, even if the probability is low. In turn, these applications can offer effective and equitable treatments to balancing risk and opportunity (Renn, 2017). Ultimately, acceptable risk shall not only be determined by probability or judgement alone. It is important for risk managers to thoroughly analyse the (low) probability of events, the subjective judgements on acceptable risks and the strength of knowledge (SoK), which support these judgements and or probabilities (Aven, 2014, p. 206).

In application towards the renewables industry: ALARP

The intention of applying the precautionary/caution principle is to decrease vulnerability and to balance protection with development by avoiding damages that may be irreversible. This method is used due to the necessity of protecting assets, people, and environment while operating in a

business area with extreme uncertainties pertaining to the development of new technologies. The renewables industry is young, and the development of relevant technologies is constantly evolving, with the future seeing increased and developing production of carbon capture, offshore wind, battery storage, biofuels, and green hydrogen among others. The success and protection of these industries are vital for forwarding the energy transition and achieving net zero by 2050; therefore, it is important that the balance between development and protection is prioritised. This value concerning the energy transition links tolerability and acceptability judgements into the ALARP model, where the specific risk shall be reduced to the lowest possible, yet achievable level or 'as low as reasonably practicable'. This is to say that the risk-reducing measures shall be applied, given that the costs are not grossly disproportionate to the obtained benefits (Langdalen et al., 2020). Tolerability will be discussed further in chapter 4.2. In the case of this thesis, when discussing security risk management in relation to malevolent actors, concerning renewable energy, the ALARP model can assist in the efficiency and protection of production, by taking into account technical, economic, and social factors.

When using the ALARP principle, verifying gross disproportion is a necessary step, although the appropriateness of using the ALARP principle depends on how gross disproportionality is interpreted. Importantly, the criteria must be interpreted differently and appropriately depending on the specific decision-making problem (Langdalen et al., 2020); (Abrahamsen & Abrahamsen, 2015). This means that the criterion and perspectives for interpretation, ranges from one extreme (economic perspective) to the other extreme (safety perspective). Focusing too heavily on one perspective will limit either growth or protection, as the economic perspective limits focus on uncertainties and the extreme safety perspective (cautionary approach) does not include reference to cost-benefit analysis.

As ALARP lies between the two perspectives, it will implement safety measures, but it will not implement them 'no matter the cost.' As stated, safety measures are implemented unless for example, the costs or operational restrictions are grossly disproportionate to benefits (Aven & Vinnem, 2007). Grossly disproportionate covers a wide spectrum of uncertainties between economic and safety perspectives, and ALARP can often vary from one extreme to the other.

Grossly disproportionate therefore depends on the decision problem and how it is interpreted, refer to Figure 2.

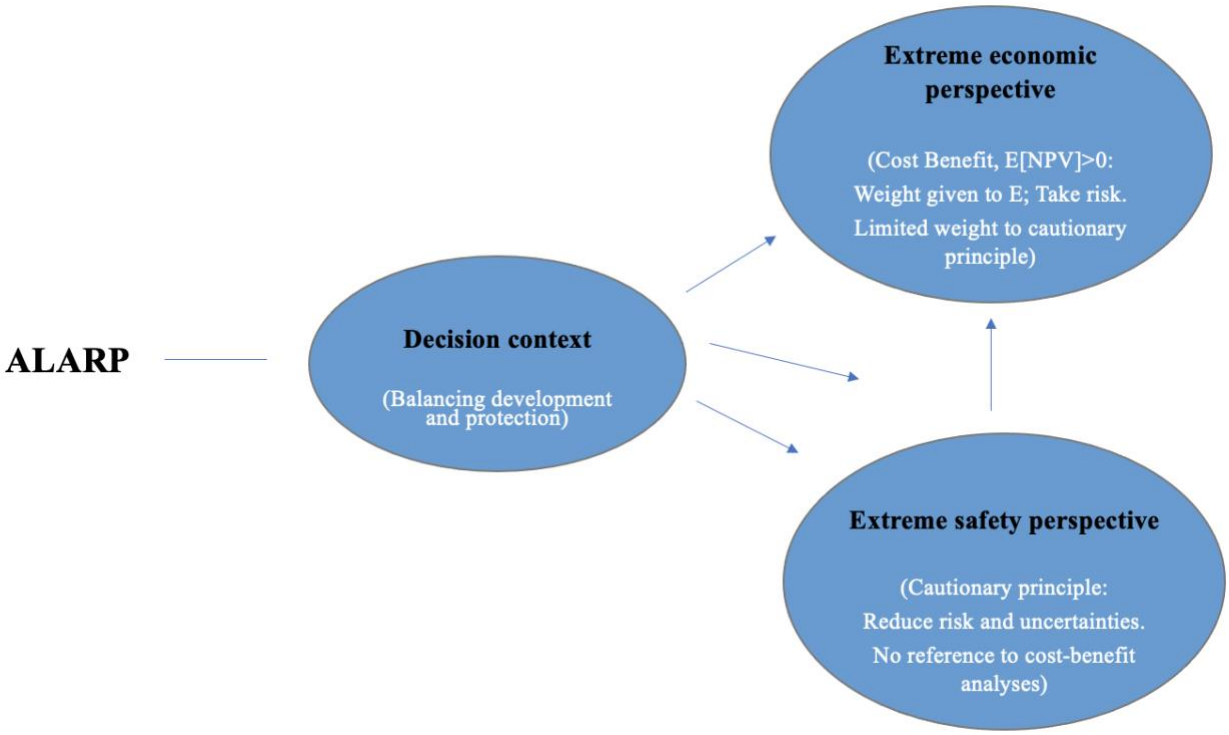

Figure 2 ALARP outline. Adapted from Aven (2014); Abrahamsen & Abrahamsen (2015)

Applying the layered approach to verify the ALARP principle is dynamic (includes uncertainties) and is therefore beneficial (Aven & Vinnem, 2007). In brief, focus is first placed on the costs, and if low, the measure will be implemented. If the costs are high, a more detailed analysis (for example cost-benefit analysis) will be carried out, and if this analysis states it is beneficial to invest, the measure will be implemented. If the expected net present value (ENPV) is negative or the expected costs are greater than the expected benefits, then focus will be placed on other issues, including uncertainties. In the end, the decision maker may or may not implement the measure, regardless of the result produced by the cost-benefit analysis. This is due to uncertainties related to the phenomena, consequences, and conditions, which consider that although the ENPV is negative (0), the actual benefit of implementing the measure may still be significant (Aven, 2011). These processes are presented in Figure 3.

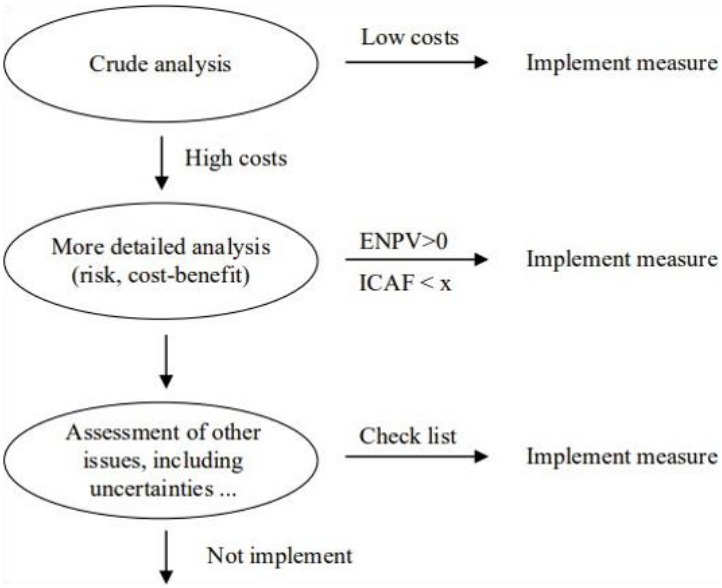

Figure 3 Layered approach to ALARP (Aven, 2011, p. 9)

Since the publishing of "Risk management with applications from the offshore petroleum industry" by Terje Aven and Jan Vinnem in 2007, the ALARP principle has been adopted within the UK oil and gas sector. It was with insight from risk experts that the same adoption should take place within the Norwegian oil and gas sector. This had been seen as the desired method, as opposed to the use of the risk acceptance criteria, which has a pre-defined regulation regime concerning risk. It is argued that by applying the ALARP approach, the link between political decisions regarding risk acceptance and the operator's risk criteria can be interwoven and the balance of power and expert understanding of risk and reward can be optimised. The argument states that by implementing the ALARP approach rather than a pre-defined risk criterion, the decision to implement a risk-reducing measure would be decided based on the balancing of benefits and burdens rather than political acceptability. With this method, it becomes the operator's responsibility to create an acceptance criterion concerning risk issues (Aven & Vinnem, 2007).

4.1.2 Risk-informed management strategies

As discussed with the ALARP principle, the framing of the safety measure depends on the decision context, in which a singular focus on one end of the extremes can lead to unintended

side effects on the other end. This logic applies to the implementation of any security or safety measure. When considering a measure in isolation, the focus on the system in its entirety is diminished, which ultimately impacts the decision-making context and the interactions between other safety or security measures. By approaching security measures and decision making through a systems approach, this limitation is hindered, and uncertainty is taken into greater consideration. The systems approach (also understood as systems thinking), is a conceptual framework that emphasises the holistic perspective of viewing the entire system and its interconnectedness, rather than focusing on isolated components (Langdalen et al., 2020).

Weighing the pros and cons, including managerial values, goals, criteria, and preferences, followed by finally choosing one course of action over another is challenging. However, it is vital that the consequences of each alternative within the system is made clear prior to the making of the final decision. Risk analysis tools such as multi-attribute analyses and Bayesian networks can assist in displaying all relevant risks, SoK assessments, and costs and benefits (Aven & Kørte, 2003). Additionally, conducting a concern assessment can provide insight into the impact of risk (positive or negative) on the socio-economic environment. Furthermore, when dealing with uncertain and complex (and or ambiguous) risk problems, it is necessary to complement information on physical consequences with that of secondary effects, this includes incorporating response to, and perceptions of risk (Renn, 2017). Ultimately, for the decision analysis, all alternatives must be assessed. These analyses are based on background information; therefore, it is important that risk-informed management strategies are prioritised by their SoK assessments. Analysing how much knowledge is available and deliberating upon what must be done in order to build this knowledge is crucial (Aven & Kørte, 2003). By adapting a systems approach, assessors establish a basis and starting point for risk-informed decision-making.

The knowledge assessment model for using the systems approach can be evaluated in light of the SEIPS model (Systems Engineering Initiative for Patient Safety) as it is a useful model for describing socio-technical systems (Sørskår et al., 2017). The model is based on the SPO framework, consisting of three elements:

1) Structure (system components, which interact and influence each other, including persons, tasks, technology).

2) Process (series of steps within the structure to generate outcome).
3) Outcome (measured in employee/organisational outcomes).

The objective is to identify and evaluate human factor principles for their process performance and quality of the outcome by identifying, structuring, and evaluating knowledge (Sørskår et al., 2019). SoK within the knowledge assessment shall therefore be determined for each knowledge element within the analysis phase, refer to Figure 4, with (3.) identifying critical knowledge elements. The system itself is holistic in its approach, by capturing both the human and technological aspect. It presents an informative risk picture to decision-makers, and it can be further applied as a feedback loop, by reporting, capturing and recording events, allowing for the management of improvements (Sørskår et al., 2017); (Sørskår et al., 2019).

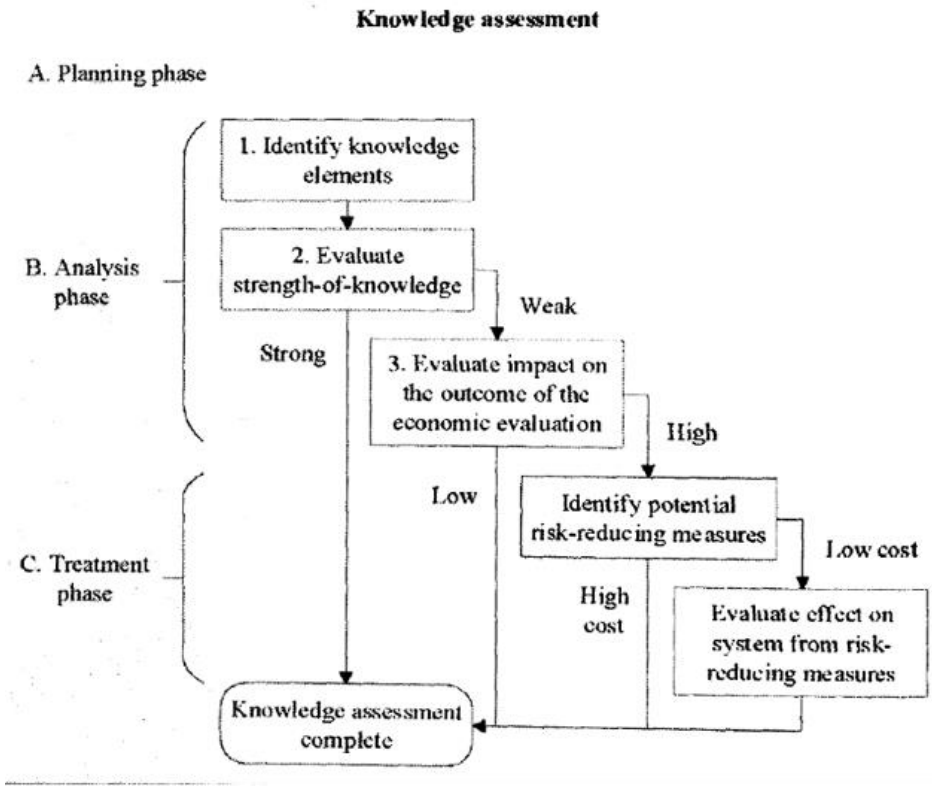

Figure 4 Suggested methodology for knowledge assessment (Sørskår et al., 2019)

When adapting a systems approach, unintended implications or side-effects can occur, such as the crowding out effect of resources, it is therefore important to take into account resource scarcity when implementing a new measure. If this is not considered, an overestimation of the

benefits of one security or safety measure could occur, resulting in a reduction in benefits from other existing measures. For example, over-investment in a new measure could result in a lack of funding to support annual employee security training. Thus, sub-optimal resource allocation and insufficient focus on the systems can lead to unintended consequences (Sørskår et al., 2017). Further limitations include the application of the ALARP principle in combination with the systems approach, as the nature of ALARP means that risk-reducing measures are typically assessed in isolation. By limiting attention and ultimately knowledge on how other safety measures interact within the system, necessary reflection upon the premise of the decision is not given. This can result in too much weight being given to either the safety perspective or economic perspective, thus resulting in the poor identification of relevant costs and benefits (Langdalen et al., 2020). Integrating these two systems is still a topic of discussion among risk experts, although in brief, systems thinking is relevant and applicable when applying the ALARP principle. Systems thinking is ultimately useful in assisting and understanding decision options regarding the safety perspective.

4.2 Company risk appetite and tolerability

Expert perception on risk tolerability from the Norwegian companies will be analysed in this chapter to determine how much residual risk the companies are currently accepting. Information pertaining to each company was acquired via interviews with heads of security at Aker ASA in coordination with Aker Horizons (Mainstream RP), Aker Solutions and Aker BP. It is the author's motive that understanding risk appetite and tolerability differences between the analysed companies will pave the way for risk assessment improvements, such as implementing tools targeted towards growth and protection incentives. As mentioned in chapter 4.1, the use of the ALARP principle is discussed due to concerns associated with growth versus protection and its linkage to risk tolerability. Moreover, the tolerability assessment will support homogeneity within the Aker chain by creating an overview of the focus areas each company prioritises. Further suggestions can then be made based on any unaddressed risks, when compared to the other analysed companies.

4.2.1 Aker Horizons (Mainstream RP)

Mainstream RP is a global pure-play renewable energy company, which is majority owned by Aker Horizons and predominantly operates in medium to high physical security threat locations. The company chooses locations based on renewable opportunity and granted operational licensing. In the future, the company will most likely continue to operate within medium to high security threat locations, although there are segments of the company's offshore wind farming which operate in low to medium security threat locations. Conclusively, Mainstream RP acknowledges that more comprehensive assessments of market challenges in higher risk locations such as South Africa, Chile, and Vietnam is desirable (refer to Table 1).

Due to the low margin nature of renewable production, the substantial investments required, and the challenge of achieving satisfactory financial returns, market dynamics are viewed as the primary threat to renewable growth. Additionally, when comparing the market capability to oil and gas, the time frame for generating income as a renewables company is more challenging and uncertain due to intensive costs and longer lead times. Therefore, it is critical that the company carefully identifies renewables sites which can offer optimal return. This underscores the importance of effectively conducting market and security assessments to promote successful expansion and long-term viability. These factors ultimately lead to a greater discussion with authorities on whether energy security should purely be a private investment or if investments should also be backed by public funding.

Aker Horizons (Mainstream RP) considers the current market and security risks in the countries of operation as both manageable and acceptable, primarily due to the presence of significant operational opportunities. However, there are certain risks that are deemed intolerable, specifically when concerning extremely unstable countries where the viability of an asset is uncertain. This perspective is reflected in strategic decisions, such as Aker ASA's choice not to proceed with the acquisition of Emergy renewables company (formerly known as NTB), in 2021. Regrettably, the wind farm owned and operated by Emergy's subsidiary, East Renewable Energy, namely The Syvash Wind Farm located in southern Ukraine near the Crimean Peninsula, was

targeted by a rocket attack at the onset of the war in Ukraine in January 2022. Consequently, Emergy projects in Ukraine are currently on hold due to the challenging geopolitical situation.

Further examples of intolerable risk include countries that face significant challenges associated with high corruption or insufficient government action in meeting their payment obligations. In such cases, the company may opt to back away from these opportunities due to the intolerable level of risk involved. Conclusively, with Mainstream RP being very opportunistic, focus is taken away from threat assessments, which could result in the oversight of obscure risk factors.

4.2.2 Aker Solutions

Aker Solutions is a project-based company and operates predominantly in low security threat locations within the Norwegian and UK continental shelf. However, as an entrepreneurial company, Aker Solutions is open to conducting business in different geographies. Recent risk reducing measures for operating in different locations, include the placing of assets located in Africa and Brazil in a joint venture with Schlumberger. This, according to Aker Solutions will result in a decrease to the company's physical security risk profile.

In terms of Aker Solutions as a procurement and construction-based company, they are closely tied to milestones with very sensitive target timeframes for contractual deliverables. Having the resources to meet milestones and deliver against aggressive timelines with heavy penalisations should milestones be missed, presents itself to be the greatest market concern for the company. In terms of dealing with the challenge of a low-margin market, the issue is combated by building close relationships with customers and creating an open dialogue about risk and how the companies expect risk to be managed. The primary security concern to renewable growth within Aker Solutions is considered insider threat and information security breaches, although activism (both physical and cyber) is a growing concern due to the company's connection to the oil and gas sector. Ultimately, when comparing market risks to malicious security risks as a threat to renewable growth, Aker Solutions weighs both equally.

Aker Solutions' risk appetite is driven by the risk appetite of their partners and customers, and they have concluded that injury to activists is an intolerable outcome. The company currently claims to be satisfied that their mitigating actions are commensurate with the risks they have identified. Furthermore, the company has examined and aligned with partnerships, including Equinor, to discern what their risk response would be should an activist led event take place on either an Aker Solutions compound or an Equinor site.

4.2.3 Aker BP

Aker BP is a pure-play upstream oil and gas company operating on the Norwegian continental shelf, thus operating in low physical security threat locations. This, however, does not hinder the increasing concern and risk associated with cyber threats. The company, as Norway's largest independent energy company, has naturally higher margins to support proactive risk-reducing measures, however, the company's risk appetite is low and there is critical analysis regarding the prioritisation of where to engage resources. On a 1 to 10 risk scale, with 1 being a low-risk appetite, 5 being a moderate risk appetite, and 10 being a high-risk appetite, the company claims to operate within areas 3 and 4: or green and yellow on a traffic light scale. This scale is supported by the company's maxim of "no incidents with serious business impacts." KPIs (key performance indicators) and maturity assessments are used to measure these scales, alongside bi-weekly meetings taking place with senior management on security risks and intelligence reports associated with relevant risks and threat indicators. Although the company accepts risk where appropriate, intolerable risk can be exemplified when it impacts licence to operate and or fatalities in the operational domain, which could result in the shutting down of operations. The company is continually and proactively working towards a future desired state to increase situational awareness and broaden understanding of security risk consequences, while simultaneously developing tools to manage the increase of industrial security threats to the energy sector.

4.3 Suggested improvements to renewable security practices

Upon analysis of Aker Horizons (Mainstream RP) and Aker Solutions annual and sustainability reports, coupled with interviews with heads of security, it is the author's incentive to bring to light relevant security practice deficiencies. By acknowledging deficiencies, suggestions for improvement concerning reporting, SRAs, and general security risk practices can take place. The risks of not proactively taking into account and managing potential security threats can lead to unwanted and surprising events. Such oversight can lead to increased costs and hinder progress towards securing the green transition and achieving carbon neutral goals. Assigning appropriate risk-reducing measures, while also supporting development goals, can be optimised by means of applying risk management tools and instruments such as the ALARP principle and the systems approach to decision making, which were discussed in chapter 4.1. The following section will analyse and advise Aker Horizons (Mainstream RP) and Aker Solutions individually, concluding with broader suggestions, applicable to all companies.

4.3.1 Aker Horizons (Mainstream RP)

Upon consultation with heads of security at Aker ASA, who support Aker Horizons in managing security risks across their renewable portfolio, it is acknowledged that there is inconsistency in the conducting of threat and risk assessments for both Aker Horizons and Mainstream RP. It is therefore recommended that the renewables companies operating internationally, specifically Mainstream RP, conduct regular threat and risk assessments for the location of operation as well as prior to making development decisions.

The result of managing risk reactively without conducting prior risk assessments can lead to further vulnerabilities to an industry which already suffers from challenging market dynamics and financial returns. Vulnerabilities to business are perpetuated by electricity price disparities, which have the capacity to induce significant cost strains should market conditions fall. Upon analysing market conditions within Chile, it was identified that the country's energy sector is particularly vulnerable to the effects of global warming and droughts due to their reliance on hydro power. In 2022, Chile failed to produce adequate levels of hydro power, resulting in a

significant increase in demand for wind power. With induced price changes and the obligation of operating wind farms to deliver power at a defined production rate or buy power from the market, Mainstream RP was exposed to the consequence of significant cost strains. An example scenario of a none-proactive risk management approach concerning security include starting developments in a country without conducting a threat assessment during the decision-making process. In countries such as Chile, the country has historically experienced higher levels of violence and corruption, making companies vulnerable to both market challenges and security issues linked to regional issues associated with tribal land disputes. Consequently, besides the acknowledgment of cyber risks, there is limited reporting and discourse within the company concerning the possibility of malicious events or actors subjecting the company to "physical" security threats. It was only through interview discussions that this subject matter was both acknowledged and recognised as requiring greater attention.

In contrast, Aker ASA and Aker Horizons exemplify a proactive approach to risk management, as demonstrated in their evaluation of the potential acquisition of Emergy renewables company, operating within Ukraine. As part of Aker ASA's risk assessment process, comprehensive screenings (IDD) were conducted on Emergy, their key personnel, and the project portfolio from 2018 to 2020. The findings indicated that the wind farm operating near the Crimean Peninsula carried a high risk, both for the project itself and the safety of personnel, making it susceptible to becoming a lost or stranded asset. Consequently, Aker ASA and Aker Horizons decided not to proceed with the acquisition, thereby avoiding both the stalling of Ukrainian operations and the loss of an asset due to current geopolitical conflicts.

In the future, Aker Horizons intends to have portfolio companies conduct assessments internally, however, as of 2023, Aker ASA has been conducting them. Disadvantageously, with Aker ASA being an investment company, they are not operating directly in the field and therefore, lack a comprehensive overview of the threat landscape, in contrast to the individual portfolio. Further identified challenges include, establishing a culture to promote risk awareness and facilitating early financial, market, and risk assessments within the portfolio. This has revealed itself to be a particular obstacle for both annual and project-based assessments. Despite the challenges in establishing this awareness, it is essential for the company to prioritise improving risk culture in

order to gain a better view of security from the ground up. In addition, it is recommended that Aker Horizons (Mainstream RP) specifies and defines the criticality of its assets, as this will help cost-effectively deploy security measures and resources when evaluating the consequences of impacts and how they affect return on investments. In comparison, Aker Solutions requires each asset location to identify what is critical for their business operations, with the owner of the asset determining the criticality of said asset. Moreover, Aker BP analyses criticality based on the criteria of availability, confidentiality, and integrity.

In conclusion, practical SRA adaptations should include country risk assessments prior to entering a country, conducting risk assessments on an annual basis, and conducting SRAs on each site. This should include a local security threat assessment with relevant threat actors in the area, history of risk in the area, and whether actors have intent to target. Vulnerability assessments should be conducted, and appropriate controls should be implemented to meet the analysed threat level. Furthermore, oversight of criticality and impact of identified security threats should be gained, and if appropriate, reported upon annually. With the current approach to security risk being reactive, the company does gain information on how to make operations more robust with time but, ultimately, it is advised to take a cautionary approach in the face of uncertainty, which will allow for learning by restricted errors (Renn, 2017).

4.3.2 Aker Solutions

It is suggested that Aker Solutions gain a better understanding of where the security department stands during their risk mitigation process. Suggestions include to improve SRA spreadsheet deficiencies. Currently the focus is heavily placed on mapping the likelihood and consequence of specific risks, with too little focus placed on mitigating actions and plans to reduce risks to acceptable levels. The aim should be to improve dialogue on risk appetite and establish indicators on what the risk appetite is and why. Improving dialogue will allow for better communication surrounding the stage in which the security team is at in terms of analysing and mitigating risk. This includes dialogues on what is enough or too little action, how much a specific risk measure would reduce exposure to a risk, or how much is needed to be spent to

reduce a risk. This shall be accompanied by determining if the security team is short on resources or if the risk has been mitigated to a tolerable level.

Within Aker Solutions, SRA's are conducted at Tier 1 ground level within the company's organisational structure and takes a hands-on approach to security incidents. As previously indicated, there is an absence of security visibility from the ground up. Improving this overview will both strengthen SRA's across the entire risk landscape and allow emergency response teams to become more closely linked to SRAs, ultimately making the teams more resilient. Currently the emergency response teams are geographically set up through the tiered approach. Tier 2 is the segment (business area) within the country of operation, and at this time many operations are segment and country based. The segments within Aker Solutions pertain to either the reorganisation of new builds or lifecycle of projects (maintenance and offshore deployment) or power solutions within the renewables sector. The concern with Norway is that there are multiple segments all operating in the same country. The goal, therefore, is to increase resilience within the individual segments and to build up emergency response teams within the two key segments operating in Norway.

Notably, with Aker Solutions growing both organically and through mergers and acquisitions (M&A), company goals will also include facilitating better coordination with M&A to understand how they conduct business and risk. This is particularly relevant if employees are travelling more frequently to facilitate business, as there needs to be an understanding of how they are going to manage risk.

4.3.3 Closing remarks on suggested improvements

In conclusion, upon analysis of chapter 3 (security comparisons), chapter 4.2 (risk appetite) and chapter 4.3.1 and 4.3.2 (individual company suggestions), it is deemed necessary to include additional, broader suggestions for consideration. These are listed as follows:

Security departments need to identify more thoroughly what their security risk appetite is, as this will assist in acknowledging relevant risks and devising appropriate measures to help balance

protection with development incentives. This can be achieved by incorporating risk characterisations into the assessment framework. Identifying risk and its characterisations will frame meaningful discussions on results of risk assessments, streamlining communication and decision-making. This thesis acknowledges risk as being broadly defined as the consequences (C) of an activity (A) and associated uncertainties (U); or (A, C, U), which can then be used to derive "general risk characterizations (A',C',Q,K), where A' is a set of specified events, C' some specified consequences, Q a measurement or description of uncertainties and K the knowledge that Q and (A',C') are based on" (Aven & Thekdi, 2021, p. 24). For more information, refer to Aven and Thekdi (2021) chapters 2 and 3.

Meaningful discussions on mitigation measures can be hindered if risk is not being properly characterised. As part of the risk characterisation, it is important to ascertain what type of consequence would result in the greatest negative impact to company values. Dynamic scenario analyses (as seen in Omny software) can be used to identify likely (intolerable) risks and consequences, and Bayesian analyses can assist in creating a visualisation of the risk characterisation. Moreover, the security department needs to have active oversight of the risk landscape to generate knowledge concerning threat, intent, capability, and impact categories. The company can then identify the areas with the highest likelihood of malicious attack and determine which company segment, asset, or infrastructure is most vulnerable and most valuable. With no other extraneous variables such as the presence of company employees', this could include focusing on assets of critical national, or company infrastructure and information. Ultimately, if the knowledge assessment suffers, so too will the decision analysis, due to a lack of basis for assessing uncertainty associated with malicious events and likely consequences.

With strong knowledge assessments, proactive conversations regarding the assignment of appropriate risk mitigating measures can then ensue to reduce risks to acceptable levels. If it is deemed critical, the implementation of measures to prevent impact should be put in place. These suggestions aim to structure and homogenise assessments, to increase robustness and reduce costs by ensuring the implementation of purely necessary security measures. Ultimately, better communication and greater knowledge generation surrounding the security risk landscape are suggested to conduct more efficient and effective risk assessments.

Chapter 5
Conclusion

This thesis had three main objectives. Firstly, to deepen understanding on the uncertain and complex market challenges faced by renewable production in various geographies of operation. Secondly, to gain a better understanding of security risk culture within renewables companies, the current security risks renewables companies face, and the methodologies they used to assess and manage security risk. Finally, by analysing these elements, this thesis aimed to offer fit-for-purpose recommendations designed in accordance with the evolving nature of both the energy sector and the security landscape.

This thesis identified that renewable energy majors require the flexibility of operating in different geographies, which have natural resource availability and diversity. This, however, necessitates operating in geographies with varying levels of bureaucratic and socio-economic stability to maximise opportunity. The consequence of instability results in the greater possibility of violence and or acts of malicious intent perpetrated by actors to achieve personal gain. Furthermore, due to both the climate crisis, issues surrounding energy security, and energy independence, the demand for renewable production is increasing. With this growth, brings increased digitalisation, advancements in R&D, and competition within technology. These elements create an attractive environment (both digital and physical) for malicious actors to target the renewables sector. It is for this reason that market risks and security risks are linked together as a starting point to frame discussions on appropriate security risk management suggestions.

As the suggestions made in this thesis are based on the uncertain and complex nature of renewable energy production, it was deemed necessary to conduct an analysis on the criteria that differentiate between simple, uncertain, complex, and ambiguous risk problems. The distinction between risk problems allowed for the designing of applicable risk strategies, based on the individual risk characteristics. This method was used as a heuristic tool to support risk management suggestions in chapter 4 and was devised in line with the IRGC Risk Governance

Framework (2005). Moreover, to gain a more extensive understanding of the specific complexities and uncertainties associated with renewable production, it was prudent to identify market risks in accordance with the locations in which the companies operate. These factors were identified in Table 1 from chapter 2.2.2.

Furthermore, to gain understanding on how the companies have been managing these security and market risks, this thesis analysed annual reports and conducted interviews with heads of security within each company. It was identified with certainty that security risks are not currently being prioritised within renewable companies. It was also concluded that due to lower margins, it is not feasible for renewables companies to implement the same degree of security measures as the offshore oil and gas industry. This thesis, therefore, focused on creating awareness and suggesting improvements to help optimise security governance within renewables companies.

The results found that focus on robust processes and resiliency through cautionary/precautionary measures and risk-informed strategies would be beneficial for application within renewable security risk assessments. Two methods were suggested: first the ALARP tool, which focuses on decreasing vulnerability to balance protection with development; and secondly, the systems approach to decision-making, which aims to more effectively implement and better understand the interactions between risk measures within complex systems.

In terms of broader risk practice improvements, chapter 4.3 presents specific suggestions tailored for each renewable company individually, as well as comprehensive recommendations for the portfolio as a whole. The analysis revealed a significant observation, being that the current state of SRAs lacks a structured approach that effectively frames and facilitates meaningful discussions on risk management. Consequently, a "poor risk assessment foundation (will) hamper effective risk communication" when it comes to decision-making (Aven & Thekdi, 2021, p. 165). To make room for good decision-making, there first needs to be an improvement to the structure of SRAs, and to improve SRAs, initiatives need to be in place, which can allow for better communication on the framing of risk issues. Only upon achieving better initial communication will improvements to renewable security risk culture and governance take place.

Conclusively, by fostering greater security risk awareness, followed by incorporating risk-informed management strategies such as risk characterisations into the SRA process, a more meaningful assessment can take place. This will enable informed decision-making and effective implementation of risk mitigating measures. These concepts were highlighted in chapter 4.3.2 and 4.3.3. Furthermore, promoting alignment and facilitating coordination among stakeholders through this approach enhances the organisation's robustness, enabling better forecasting and resiliency against disruptions. Strategically, this approach enables companies to seek more opportunities in higher risk geographies and improve efficiency in the long run. Notably, the Omny software, discussed in chapter 3.1.2 represents a transformative advancement in cyber security risk management, and includes many desirable parameters to measure risk. Going forward, tools such as these can be used to help reduce the time and resources necessary to produce results on security risks.

This thesis is limited by the constraints of analysing only four companies within the same portfolio, which limits generalisability. Analysing a more diverse sourcing pool would be beneficial in future research, however, the challenge lies in navigating privacy and confidentiality regulations, which hinder the access to necessary information. Furthermore, limits to chapter 3 and 4 comparisons are subject to the differences in reporting styles, differences between interpretation of interview questions, and the amount of information comfortably offered by each individual company.

In turn, the advantage of designing this thesis as a comparative analysis was the ability to gain a better understanding of the differences in security risk culture between sectors. Additionally, considering that a uniform understanding of security risk is desired across the Aker chain, comparing the security approaches in this thesis serves as a valuable means of facilitating effective communication and information exchange. It assisted in creating a visual representation of missing links and areas in need of improvement. It is the author's hope that this thesis can be a starting point for renewables companies to begin incorporating principles of security risk governance from oil and gas, but to adapt the process to suit renewables.

The risk comparisons in this thesis aimed to inform suggestions and highlight differences in risk governance and practices among the companies, rather than prescribing specific risk-measures. It is therefore advised that to amplify homogeneity, while also cultivating a better risk culture, improved risk communication guidelines should be implemented within each company. Going forward this will strengthen SRAs, create meaningful dialogue between analysts and decision-makers, and enforce the necessary shift in renewable security risk management. Conclusively, further analysis concerning improvements to risk communication within the renewable energy sector can be an important direction for future research. This research can explore more deeply the discursive strategies aimed at addressing ambiguous risk problems, where consensus on values vary and may impact cohesive, transparent, and homogenous dialogue between stakeholders.

Appendixes

Appendix A

Company renewable market landscape

In reference to Chapter 2.2.2 Table 1

Sources:
Mainstream RP and Aker Solutions websites and recent annual reports: (Aker Mainstream Renewables AS, 2023); (Mainstream Renewable Power, 2022); (Aker Horizons ASA, 2022); (Aker Solutions ASA, 2022b); (Aker Solutions ASA, 2023c); (Aker Solutions ASA, 2023a)

*n/a: not available

Table 11 Mainstream Renewable Power – Europe Market Landscape

Location: Europe	Type of Asset	Position in Market Landscape	Ownership and Status	Criticality (energy output)
UK: **Scotland** **England**	Offshore wind Offshore wind	Projects in operation or construction represent 20% of UK's offshore wind capacity.	One site sold and one secured for development. One site sold and in early development/ consenting phases.	50 GW target operational by 2030; 375,000 homes already powered/year. Potential for 1.8 GW; Expected to power the equivalent of over 2 million homes.
Ireland	Offshore wind	To support the Government's 2030 emissions targets for the electricity sector by 2030.	Three sites sold and in development.	7GW by 2030.
Norway	Offshore wind	n/a.	Two areas for the 2025 licencing round.	Total capacity of 4.5 GW. 30 GW by 2040.
Sweden	Offshore wind	Site locations will be in near proximity to cities and industry, which require significant amounts of energy.	Exploring four sites for floating and fixed bottom offshore wind.	n/a.

Table 12 Mainstream Renewable Power – Latin America Market Landscape

Location: Latin America	Type of Asset	Position in Market Landscape	Ownership and Status	Criticality (energy output)
Chile	Onshore wind Solar Ammonia production facility	Mainstream RP is the largest renewable energy company in Chile.	Onshore wind assets: three sold, two in construction, five owned and operated by third party. Solar assets: three in operation. Feasibility studies being conducted as of 2022.	Wind: 2.2 GW total net capacity. Solar total: 0.6 GW total net capacity, 433,000 tCO_2e avoided/year, 433,000 powered homes/year. Ammonia: Up to 1,500-3,000 MW of electrolyser capacity.
Colombia	Onshore wind Solar	n/a.	Onshore wind assets: one in development. Solar assets: one in development.	Wind: 380 MW in development. Solar: 480 MW in development.

Table 13 Mainstream Renewable Power – Africa Market Landscape

Location: Africa	Type of Asset	Position in Market Landscape	Ownership and Status: all sold	Criticality
Egypt	Onshore wind	Largest operational wind farm in the Lekela Power portfolio. 20-year PPA.	One asset owned and operated by third party.	1,000 GWh+ electricity yearly and will power 350,000 homes annually. Estimated reduction of 550,000 tCO_2e yearly.
Ghana	Onshore wind	n/a.	One asset in advanced stage development.	150 MW at start, with potential to add 75 MW.
Senegal	Onshore Wind	Provides 15% increase in energy capacity to country. 20-year PPA.	One asset owned and operated by third party.	450,000 MWh of electricity per year to more than two million people.

South Africa	Onshore wind Solar	Mainstream RP is the leading Renewable company in South Africa; 850 MW already delivered into operation.	Onshore wind assets: in development, with one developed and sold, and five sold to joint venture company, Lekela Power, and operated by Mainstream RP. Solar asset: in development, with two developed and sold, and six with signed PPAs.	Wind: 6.1 GW in development Mainstream RP operates over 600 MW for Lekela Power. Solar: 7 GW in development. Current combined capacity of 450 MW.

Table 14 Mainstream Renewable Power – Asia Pacific Market Landscape

Location: Asia Pacific	Type of Asset	Position in Market Landscape	Ownership and Status	Criticality
Australia	Solar Hybrid wind Battery co-locating	Currently exploring opportunities.	n/a.	1.0 GW estimated capacity.
Vietnam	Offshore wind Solar	The Phu Cuong Soc Trang offshore wind farm (1.4 GW) will be SE Asia's largest upon completion. Mainstream is the leading developer in the country.	Offshore wind assets: two in development. Solar assets: one in development.	Wind: 1.9 GW offshore wind in development. To power 1.6m+ homes & prevent 1.8MtCO_2e+/year. Solar: 405 MW solar portfolio in development.
Philippines	Onshore wind	Project to support government's sustainability agenda with 35% electricity coming from renewables by 2030 and 50% by 2040.	One asset in development.	90 MW wind project in development.
South Korea	Offshore wind	A milestone in the development of one of the world's first large-scale commercial floating wind farms. KF Wind will consist of 75 floating turbines.	One asset in development.	1.2 GW total capacity 4,000+ GW/h electricity generated each year. 3.18MtCO_2e avoided/year.
Japan	Offshore wind	Potential future market.	n/a.	n/a.

Table 15 Aker Solutions – Global Market Landscape

Location	Type of Asset	Position in Market Landscape	Customer	Criticality (energy output)
Norway	Offshore wind (Hywind Tampen)	Hywind Tampen is world's largest floating offshore wind project.	Equinor	Hywind Tampen aims to reduce CO_2 emissions by an estimated 200,000 metric tons per year. It is anticipated to cut up to 500,000 metric tons of CO_2 emissions annually.
	Electrification (Troll West)	n/a.	Equinor	Troll West will capture up to 400,000 metric tons of CO_2 annually.
	Carbon capture (Norcem)	n/a.	Aker Carbon Capture	Capacity to capture 400,000 metric tons of CO_2 per year.
	Carbon storage (Northern Lights)	The Northern Lights project is crucial in expanding the market for the development of carbon capture projects in Europe.	Equinor	Potential for 1000 years of carbon storage.
UK	Offshore bottom fixed wind (Norfolk; East Anglia THREE)	Norfolk will be one of the largest offshore installations globally upon completion.	Vattenfall	Norfolk has a planned capacity of 3.6 gigawatts.
			ScottishPower	East Anglia THREE has a planned installation capacity of up to 14000 MW.
	Carbon capture (Net Zero Teesside Power)		BP & partners	Electrical output of 860 MW/ year.
USA	Offshore bottom fixed wind (Sunrise Wind)	One of the largest offshore wind farms in the US.	Ørsted & Eversource	924 MW production to power 600,000 homes by 2025.
Australia	Subsea gas compression (Jansz-lo)	World's largest subsea gas compression project.	Chevron	Large reduction in energy consumption by 20% - 60% annually. Significantly reduces emissions compared to topside option. Reduces use of steel.

In-text citations for Table 1

Chapter 2.2.2 sources

Norway	(Norwegian Ministry of Petroleum and Energy, 2016); (NOU 2015: 15, 2015); (Ministry of Climate and Environment & Ministry of Foreign Affairs, 2021); (Aker Horizons ASA, 2023)
Sweden	(Ministry of the Environment and Energy, 2020); (Jacques Delors Institute, 2022)
UK: **England** **Scotland**	(UK Department for Business Energy & Industrial Strategy & Skidmore, 2019); (Department for Energy Security and Net Zero et al., 2020); (Scottish Government, 2023)
Ireland	(Department of Communication, 2021); (Government of Ireland, 2023)
USA	(National Conference of State Legislatures, 2021); (U.S. Department of Energy, 2021); (Croce et al., 2011)
Australia	(Department of Climate Change, 2022); (Australian Office of Financial Management, 2022)
South Korea	(Mainstream Renewable Power, 2023); (Ministry of Foreign Affairs, n.d.); (Ministry of Trade, 2021); (Green Energy Strategy Institute et al., 2022)
Japan	(Aker Horizons ASA, 2023); (The Government of Japan, 2022)
Vietnam	(Socialist Republic of Viet Nam, 2021); (DEA & EREA, 2022); (The International Partners Group, 2022a); (UK Government, 2021b)
Philippines	(IEA, 2022c); (Department of Energy Philippines, 2021); (Bangko Sentral NG Pilipinas, 2022)
Chile	(Aker Horizons ASA, 2023); (IEA, 2022b); (energiE & MRC, 2022); (Larraín, 2022); (Ministry of Finance, 2019); (UK Government, 2021a)
Colombia	(Colombian Government, 2021); (USAID, 2022); (Climate Investment Fund, 2023); (UK Government, 2018)
Egypt	(Moharram et al., 2022); (International Renewable Energy Agency, 2018); (IEA, 2022a)
Ghana	(IEA, 2022a); (Ministry of Energy, n.d.); (Ministry of Energy, 2019)
Senegal	(IEA, 2022a); (IEA, 2022b); (Apfel, 2022)
South Africa	(IEA, 2022b); (The International Partners Group, 2022b); (The Presidency Republic of South Africa, 2023)

Appendix B

Reporting summaries of security practices between the companies

Chapter 3.1.1 categories explained

Company:	**Aker BP (Oil and gas production)**
Sources:	(Aker BP ASA, 2022a), (Aker BP ASA, 2022b), (Aker BP ASA, 2023a), (Aker BP ASA, 2023b)
Relevant notes:	- Business units are accountable for decision-making and funding governance and risk security barriers and controls, as per the financial authorisation matrix (Aker BP ASA, 2022b). - Risk matrix: consequence categories for personnel, environment, financial, reputation, and project cost. - Out of three levels: 2022 security offshore had been increased from level 1 to 2. Level 2 will eventually be deemed the new normal (Aker BP ASA, 2023b).
ERM (Enterprise risk management) framework:	- All major risks are regularly identified and communicated via the ERM process.
HSSE (Health Safety Security Environment) and SEAC (Safety and Environmental Assurance Committee):	- SEAC assures that the HSSE work is adequately and properly organised and addressed throughout the entire company. - Reviews all operational and cyber risk. - For further information, review Aker BP Annual Report (2022, p. 42).
Security Management System (SMS):	- SMS handles identification, monitoring, analysis, and management of security risk. This process is coupled with the Risk & Barrier principles.
Barrier management framework (BMF):	- Incorporated into all business areas to establish, monitor, and maintain barriers. Aim is to reduce probability of incident and impact of potential consequences. 2021 saw an increased effort to improve the barrier framework (Aker BP ASA, 2022a). - Through this framework, any residual risk is quantified and verified to be within Aker BP's risk acceptance criteria (Aker BP ASA, 2023b).
Emergency Preparedness and Response (EPR) methodology:	(Aker BP ASA, 2022b) - Risk/scenario-based framework - Materialised security risks are handled through EPR. - Provides training and handling of critical events and is designed to safeguard life, environment, assets, and reputation.
Business Management System (BMS) and Three lines of assurance:	- Framework for creating and sustaining value, trust, and predictability - BMS describes how Aker BP works, controls risk, and improves (Aker BP ASA, 2023a).

Three lines of assurance:	- To identify and respond to risk during all phases of production and operations. - Risk-based assurance of conformity to the BMS requirements is governed by the company's "Three lines of assurance" (Aker BP ASA, 2023a). - Risk-based assurance is in place to guarantee that requirements/conformity within risk management tools, measures and procedures are met, via three degrees of independency between auditor and auditee (Aker BP ASA, 2023a).
TCFD (Task Force on Climate-related Financial Disclosures):	- Groups climate-related risks into TCFD categories. - Employs scenario analysis to assess climate change and transition related impacts.

Company:	**Aker Solutions (Oil/Gas and Renewables engineering)**
Sources:	(Aker Solutions ASA, 2023a), (Aker Solutions ASA, 2023b), (Aker Solutions ASA, 2023c), (Aker Solutions ASA, 2023d), (The Governance Group AS, 2021)
Relevant notes:	- During 2022, 157 security cases were reported with most cases related to physical security, with 147 cases reported as low risk. There were no reported serious security incidents in 2022 (Aker Solutions ASA, 2023c). - The risk management process is standardised across all projects through a 'one size-fits all' approach. - Central logging system (SIEM) and the 24/7 Security Operations Centre enable Aker Solutions to detect and act on any incidents effectively and immediately (Aker Solutions ASA, 2023c).
ERM (Enterprise risk management) and TCFD (Task Force on Climate-related Financial Disclosures) framework:	- ERM manages how the organisation identifies, assesses, and manages climate related risks. - Climate (market) related transition risks are categorised as top risks and are identified and assessed as part of the overall ERM framework, which consist of risk appetite, risk governance, tools, processes, and metrics (The Governance Group AS, 2021, p. 8). - Each business segment reports their risks to ERM. - Aker Solutions maps climate-related risks in accordance with TCFD guidelines to improve resilience towards risks associated with the energy transition and physical climate risks. - Identified climate-related risks via scenario analysis exercises are incorporated into the ERM system. - Impact and risk definition: revenue loss above NOK 500 m, and / or above NOK 50 m in EBITDA (Earnings Before Interest, Taxes, Depreciation and Amortisation). Additionally, quantifiable indicators measure how the risk impacts financial value, customer value, internal processes, and people and organisation (Aker Solutions ASA, 2023d, p. 10).

HSSE (Health Safety Security Environment):	- HSSE risks are a category within the ERM procedure. Security includes physical security threats and crisis management. - HSSE is the system used to prevent harm to people, assets, and environment. - Monitors any developments in the working environment as well as implementation and maintenance of the ERM framework within each discipline (Aker Solutions ASA, 2023c). - Regular emergency response exercises conducted at all three levels of the organisation. All findings and incidents (including physical, personnel, and IT security) are registered in the Synergi tool within HSSE function.
Emergency Preparedness and Response (EPR) framework (and (CERT) Corporate Emergency Response Team):	- Determines the company's risk landscape and coordinates actions across tactical, operational, and strategic levels within the organisation (Aker Solutions ASA, 2023a). - Analyse and act upon the operational impact of cyber-attacks and coordinating emergency responses across the business. - The structure for handling unwanted events is based on a three-tiered approach.

Company	**Aker Horizons (Mainstream RP) (Renewable Production)**
Sources:	(Aker Horizons ASA, 2022), (Aker Horizons ASA, 2023), (Mainstream Renewable Power, 2022), (Aker Mainstream Renewables AS, 2023)
Relevant notes:	- Aker Horizons adopted and implemented its risk management procedure in 2022. - Physical risks are associated with effects of extreme weather or chronic climate change on assets. Focus on weather related risks have incentivised the company to build resilient assets, ultimately driving down total cost of physical risk exposure. - The quarterly risk review includes 1) assessing changes in estimated impact/probability of known risk; 2) identifying new risks with proposed mitigating actions; and 3) evaluating progress of existing mitigating actions and potential need for additional measures. - Aker Horizons assesses, monitors, and offers robust support of its own and its portfolio companies' exposure to climate-related risks and opportunities. - Project management and operation risk is the responsibility of Mainstream RP, not Aker Horizons. - Scenario analysis used to assess climate-related ramification based on specific trends and conditions. - Stress-testing is used to assess the portfolio and its investments against various climate-related scenarios and consequences of likely future outcomes amidst uncertain conditions.
GDS (Global Development Standard):	- Aim: de-risk opportunities (onshore wind, offshore wind and solar, stakeholder management and social licensing, as well as managing ERM, which uses "best practices" for the company. - Central to company's risk management framework and climate-risk

	management. - Updated annually.
ERM (Enterprise risk Management):	- For identifying, reporting, and providing tools to manage all material risk. - All major risks are identified, reported, and assessed via the ERM process. Risks are analysed in four broad enterprise-level risk categories. These categories consist of climate risk, encompassing strategic and market risk (Transition risk), and Project and operational risk (Physical risk). Utilising a provided template, the portfolio companies are required to identify a minimum of three and a maximum of ten key risks for each category (Aker Horizons ASA, 2023, p. 194) - Specific criteria are required for managing and reporting risk at the board level.
Project portfolio management (PPM):	- PPM is utilised to document risks that may cause project delays, exceed budget, or impede the project from achieving fully consented status. PPM also facilitates a holistic risk management approach by tracking project issues and metrics (Mainstream Renewable Power, 2022). - "Provides the tools that project managers require to effectively carry out Risk, Issue, Schedule, and Metric Management" (Aker Mainstream Renewables AS, 2023, p. 34).
TCFD (Task Force on Climate-related Financial Disclosures):	- Mainstream RP adheres to the TCFD recommendations regarding governance, risk, strategy, and handling of climate-related risks. - TCFD Investment Committee: performs risk assessments on investment decisions for new projects and climate risk mitigation investments. - TCFD Sustainability Committee: assesses climate change and its impact on business development.
HSSE (Health Safety Security Environment):	- Does not include cyber security - Annual report emphasises health and safety with no mention of security.

Appendix C

Interview transcript

For Aker Solutions, Aker BP, Aker Horizons (Mainstream RP)

**Renewables specific questions*

Threat Questions

1. Threat and impact categories
    a. What are the company threat categories?
    b. What are the company impact categories?
    c. What are the company threat actor capability and intent categories?
2. Is there a country security threat ranking available for locations and operations of all assets?
3. How are security incidents being managed?
    a. Are both oil/gas and renewable assets being managed in the same way? *
4. What is defined as a critical asset (how are assets prioritise and is it weighed against specific criteria?)

SRA questions

1. What is the companies SRA process?
2. Is the process the same or different for physical and cyber risks?
3. What risk concepts/principles/methods/tools are used when conducting a security risk assessment or when implementing a security measure?
    a. How does the company decide upon a security measure? What considerations are taken?
4. Cost of security for oil/gas assets are substantial but justified. Do we bring the oil/gas approach to renewables, or is it too expensive? *
5. How does the company intend to adapt/improve its security practices/ risk analysis tools/ SRAs?

Market questions*

1. How is the company combating the issue of a low-margin business?
2. Does the company plan on operating in different geographies (with higher threats or worse market conditions)?
    a. What considerations are taken when pursuing renewable operations within a country?
3. Is the threat to renewable growth greater due to the market dynamics or above ground (physical)/cyber security risks?
4. What main market challenges are the company facing?

Risk tolerability questions

1. What is the company's risk appetite (perceptions on intolerable and acceptable risk)?
    a. How much market and security risk are the company willing to accept and how much are they currently tolerating?

References

Abrahamsen, H. B., & Abrahamsen, E. B. (2015). On the appropriateness of using the ALARP principle in safety management. *Taylor & Francis Group*. https://doi.org/10.1201/B19094-104

Aker ASA. (2022). *This is Aker Security [PDF file]*.

Aker BP ASA. (2022a). *Aker BP Sustainability Report 2021*. Aker BP ASA. https://akerbp.com/wp-content/uploads/2022/03/aker-bp-sustainability-report-2021.pdf

Aker BP ASA. (2022b). *Policy Security*. Aker BP ASA. https://akerbp.com/policy/security-policy-principles/

Aker BP ASA. (2023a). *Aker BP Annual report 2022*. Aker BP ASA. https://akerbp.com/wp-content/uploads/2023/03/aker-bp-annual-report-2022.pdf

Aker BP ASA. (2023b). *Aker BP Sustainability Report 2022*. Aker BP ASA. https://mb.cision.com/Public/1629/3739884/938826d06d79be79.pdf

Aker Horizons ASA. (2022). *Aker Horizons Annual and Sustainability Report 2021*. Aker Horizons ASA. https://akerhorizons.com/wp-content/uploads/AnnualandSustainabilityReport2021.pdf

Aker Horizons ASA. (2023). *Aker Horizons Annual and Sustainability Report 2022*. Aker Horizons ASA. https://akerhorizons.com/wp-content/uploads/2023/03/Aker-Horizons-Annual-and-Sustainability-Report-2022.pdf

Aker Mainstream Renewables AS. (2023). *Mainstream Renewable Power Sustainability Report 2022*. Aker Mainstream Renewables AS. https://bit.ly/3V9d33w

Aker Solutions ASA. (2022a). *Aker Solutions Annual Report 2021*. Aker Solutions ASA. https://www.akersolutions.com/globalassets/huginreport/2021/annual-report-2021.pdf

Aker Solutions ASA. (2022b). *Aker Solutions Sustainability Report 2021*. Aker Solutions ASA. https://www.akersolutions.com/globalassets/sustainability/sustainability-report-2021.pdf

Aker Solutions ASA. (2023a). *Aker Solutions Annual Report 2022*. Aker Solutions ASA. https://www.akersolutions.com/globalassets/huginreport/2022/annual-report-2022.pdf

Aker Solutions ASA. (2023b). *Aker Solutions Corporate Governance Report 2022*. Aker Solutions ASA. https://www.akersolutions.com/globalassets/investors/agm/2023/corporate-governance-report-2022.pdf

Aker Solutions ASA. (2023c). *Aker Solutions Sustainability Report 2022*. Aker Solutions ASA. https://www.akersolutions.com/globalassets/sustainability/sustainability-report-2022.pdf

Aker Solutions ASA. (2023d). *Climate-related Scenario Analysis & Risk Assessment In accordance with TCFD recommendations*. Aker Solutions ASA. https://www.akersolutions.com/globalassets/sustainability/aker_solutions_climate_risks_tcfd_march2023.pdf

Apfel, D. (2022). Renewable energy transition in Senegal? Exploring the dynamics of emerging paths to a sustainable energy system. *Energy research & social science*, *92*, 102771. https://doi.org/10.1016/j.erss.2022.102771

Australian Office of Financial Management. (2022). *Australian Government Climate Change commitments, policies and programs*. Australian Government. Retrieved from https://www.aofm.gov.au/media/967

Aven, T. (2011). *Quantitative Risk Assessment: The Scientific Platform*. Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9780511974120

Aven, T. (2014). *Risk, Surprises and Black Swans: Fundamental Ideas and Concepts in Risk Assessment and Risk Management*. London: Routledge. https://doi.org/10.4324/9781315755175

Aven, T., Ben-Haim, Y., Andersen, H. B., Cox, T., Droguett, E. L., Greenberg, M., Guikema, S., Kröger, W., Renn, O., Thompson, K. M., & Zio, E. (2018). *Society for Risk Analysis Glossary*. S. f. R. Analysis. https://www.sra.org/wp-content/uploads/2020/04/SRA-Glossary-FINAL.pdf

Aven, T., & Kørte, J. (2003). On the use of risk and decision analysis to support decision-making. *Reliability engineering & system safety*, *79*(3), 289-299. https://doi.org/10.1016/S0951-8320(02)00203-X

Aven, T., & Renn, O. (2020). Some foundational issues related to risk governance and different types of risks. *Journal of risk research*, *23*(9), 1121-1134. https://doi.org/10.1080/13669877.2019.1569099

Aven, T., & Thekdi, S. (2021). *Risk Science : An Introduction*. Taylor & Francis Group. https://doi.org/10.4324/9781003156864

Aven, T., & Vinnem, J. E. (2007). Risk Management: With Applications from the Offshore Petroleum Industry. In *Springer series in reliability engineering* (1. Aufl. ed., pp. 50-51). London: Springer Verlag London Limited. https://www-vlebooks-com.ezproxy.uis.no/Product/Index/607061?page=0&startBookmarkId=-1

Bangko Sentral NG Pilipinas. (2022). *The Philippine Sustainable Finance Roadmap*. Bangko Sentral NG Pilipinas. Retrieved from https://www.bsp.gov.ph/Regulations/Issuances/2022/CL-2022-011.pdf

Boin, A., Ekengren, M., & Rhinard, M. (2020). Hiding in Plain Sight: Conceptualizing the Creeping Crisis. *Risk, Hazards & Crisis in Public Policy*, *11*(2). https://doi.org/10.1002/rhc3.12193 (Wiley Periodicals, Inc)

Climate Investment Fund. (2023). *CIF Approves $70 Million to Accelerate Colombia's Integration of Clean Energy Into the Power Grid* https://www.cif.org/news/cif-approves-70-million-accelerate-colombias-integration-clean-energy-power-grid

Colombian Government. (2021). *E2050 Colombia's long-term climate strategy to meet the Paris Agreement*. Ministry of Environment, DNP, Foreign Affairs Ministry, AFD, Expertise France, WRI: Bogotá. Retrieved from https://e2050colombia.com/wp-content/uploads/2022/04/Resumen-Ejecutivo-E2050-Ingles.pdf

Croce, R. D., Kaminker, C., & Stewart, F. (2011). *The role of pension funds in financing green growth initiatives*. O. Publishing. https://www.oecd.org/pensions/private-pensions/49016671.pdf

Dalby, S. (2017). Environmental (in)security. *The International Encyclopedia of Geography.* https://doi.org/10.1002/9781118786352.wbieg0428

de Arce, M. P., & Sauma, E. (2016). Comparison of Incentive Policies for Renewable Energy in an Oligopolistic Market with Price-Responsive Demand. *The Energy journal (Cambridge, Mass.)*, *37*(3), 159-198. https://doi.org/10.5547/01956574.37.3.mdea

DEA, & EREA. (2022). *Vietnam Energy Outlook Report 2021*. Danish Energy Agency, Electricity and Renewable Energy Authority in Viet Nam. Retrieved from https://ens.dk/sites/ens.dk/files/Globalcooperation/vietnam_energy_outlook_report_2021_english.pdf

Department for Energy Security and Net Zero, Prime Minister's Office, 10 Downing Street, Department for Business Energy & Industrial Strategy, Sharma, A., & Johnson, B. (2020). *The Ten Point Plan for a Green Industrial Revolution*. UK Government. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/936567/10_POINT_PLAN_BOOKLET.pdf

Department of Climate Change, Energy, the Environment and Water. (2022). *Annual Climate Change Statement 2022*. Australian Government. Retrieved from https://www.dcceew.gov.au/sites/default/files/documents/annual-climate-change-statement-2022.pdf

Department of Communication, Climate Action & Environment,. (2021). *National Energy & Climate Plan 2021-2030*. Government of Ireland. Retrieved from https://energy.ec.europa.eu/system/files/2020-08/ie_final_necp_main_en_0.pdf

Department of Energy Philippines. (2021). *2020-2040 Philippine Energy Plan* (2719 - 1443). Department of Energy Philippines. Retrieved from https://www.doe.gov.ph/sites/default/files/pdf/pep/PEP%202022-2040%20Final%20eCopy_20220819.pdf

energiE, & MRC. (2022). *Roadmap for the Energy Transition in Chile*. energiE & MRC. Retrieved from https://www.enel.cl/content/dam/enel-cl/conoce-enel/transicion-energetica/Roadmap-for-the-Energy-Transition-in-Chile-Final-Report.pdf

Government of Ireland. (2023). *Climate Action Plan 2023 CAP23*. Government of Ireland. Retrieved from https://www.gov.ie/pdf/?file=https://assets.gov.ie/256997/b5da0446-8d81-4fb5-991e-65dd807bb257.pdf#page=null

Green Energy Strategy Institute, Institute for Green Transformation, NEXT Group, & Agora Energiewende. (2022). *2050 Climate Neutrality Roadmap for Korea K-Map Scenario*. Green Energy Strategy Institute, Institute for Green Transformation, NEXT Group, & A. Energiewende. https://static.agora-energiewende.de/fileadmin/Projekte/2021/2021_04_INT_Korea_Map/K-Map_EN_final.pdf

IEA. (2022a). *Africa Energy Outlook 2022*. IEA. https://www.iea.org/reports/africa-energy-outlook-2022

IEA. (2022b). *Clean Energy Transitions Programme Annual Report 2022*. International Energy Agency. https://iea.blob.core.windows.net/assets/f75d4c63-e29d-476a-8fc7-497439d6d242/CETPAnnualReport2022.pdf

IEA. (2022c). *Southeast Asia Energy Outlook 2022*. IEA. https://iea.blob.core.windows.net/assets/e5d9b7ff-559b-4dc3-8faa-42381f80ce2e/SoutheastAsiaEnergyOutlook2022.pdf

International Renewable Energy Agency. (2018). *Renewable energy outlook: Egypt*. International Renewable Energy Agency. https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2018/Oct/IRENA_Outlook_Egypt_2018_En.pdf

Jacques Delors Institute. (2022). *The Swedish energy transition*. Notre Europe. https://institutdelors.eu/wp-content/uploads/2022/09/PB_220905_The-Swedish-energy-transition_Thalberg_EN.pdf

Kim, J., & Park, K. (2016). Financial development and deployment of renewable energy technologies. *Energy economics*, *59*, 238-250. https://doi.org/10.1016/j.eneco.2016.08.012

Langdalen, H., Abrahamsen, E. B., & Selvik, J. T. (2020). On the importance of systems thinking when using the ALARP principle for risk management. *Reliability engineering & system safety*, *204*, 1-. https://doi.org/10.1016/j.ress.2020.107222

Larraín, M. (2022). *The Roadmap for Facing Climate-related Risks of the Financial Market Commission*. Financial Market Commission of Chile. https://www.cmfchile.cl/portal/prensa/615/articles-50356_presentacion_mlarrain.pdf

Mainstream Renewable Power. (2022). *Mainstream Sustainability Report 2021*. Mainstream Renewable Power. https://www.mainstreamrp.com/f/50184/x/a507780a45/mainstream-sustainability-report-2021_final.pdf

Mainstream Renewable Power. (2023). *South Korea*. Mainstream Renewable Power. https://www.mainstreamrp.com/markets-projects/asia-pacific/south-korea/

Ministry of Climate and Environment, & Ministry of Foreign Affairs. (2021). *Norway to double climate finance to NOK 14 billion* https://www.regjeringen.no/en/aktuelt/norway-to-double-climate-finance-to-nok-14-billion/id2881477/

Ministry of Energy. (2019). *Ghana Renewable Energy Master Plan*. Government of Ghana. Retrieved from http://www.energycom.gov.gh/public-notices?limit=1&start=14

Ministry of Energy. (n.d.). *National Energy Transition Framework (2022-2070)*. Government of Ghana. Retrieved from https://www.energymin.gov.gh/sites/default/files/2022-11/National%20Energy%20Transition%20Framework%20Abridged%20Version.pdf

Ministry of Finance. (2019). *Chile: Financial Strategy on Climate Change*. Government of Chile. Retrieved from https://cambioclimatico.mma.gob.cl/wp-content/uploads/2020/12/Financial-Strategy-on-Climate-Change-Chile-EN.pdf

Ministry of Foreign Affairs. (n.d.). *Policy Information: Energy*. Republic of South Korea. Retrieved from https://www.mofa.go.kr/eng/wpge/m_5657/contents.do

Ministry of the Environment and Energy. (2020). *Sweden's draft integrated national energy and climate plan*. Government Offices of Sweden. Retrieved from https://www.government.se/contentassets/e731726022cd4e0b8ffa0f8229893115/swedens-draft-integrated-national-energy-and-climate-plan/

Ministry of Trade, Industry, and Energy. (2021). *Third Energy Master Plan*. Republic of South Korea. Retrieved from https://www.etrans.or.kr/ebook/05/files/assets/common/downloads/Third%20Energy%20Master%20Plan.pdf

Moharram, N. A., Tarek, A., Gaber, M., & Bayoumi, S. (2022). Brief review on Egypt's renewable energy current status and future vision. *Energy reports*, *8*, 165-172. https://doi.org/10.1016/j.egyr.2022.06.103

National Conference of State Legislatures. (2021). *State Renewable Portfolio Standards and Goals*. National Conference of State Legislatures. Retrieved from https://www.ncsl.org/energy/state-renewable-portfolio-standards-and-goals

Norwegian Ministry of Petroleum and Energy. (2016). *Power supply and the electricity grid*. (977 161 630). Government of Norway. Retrieved from https://www.regjeringen.no/en/topics/energy/the-electricity-grid/power-supply-and-the-electricity-grid/id2353792/

NOU 2015: 15. (2015). *Environmental Pricing (Summary) — Report from a Green Tax Commission*. Norwegian Ministry of Finance. https://www.regjeringen.no/en/dokumenter/nou-2015-15/id2465882/

Renn, O. (2017). Risk governance : coping with uncertainty in a complex world. In (1st. ed., pp. 178-180). Routledge. https://www-taylorfrancis-com.ezproxy.uis.no/books/mono/10.4324/9781849772440/risk-governance-ortwin-renn

Sandeman, J. (2010). Feed-In Tariffs: Accelerating the Deployment of Renewable Energy. *International Journal of Environmental Studies*, *67*(3), 463-463. https://doi.org/10.1080/00207230701737011

Scottish Government. (2023). *Draft Energy Strategy and Just Transition Plan*. Scottish Government. Retrieved from https://www.gov.scot/binaries/content/documents/govscot/publications/strategy-plan/2023/01/draft-energy-strategy-transition-plan/documents/draft-energy-strategy-transition-plan/draft-energy-strategy-transition-plan/govscot%3Adocument/draft-energy-strategy-transition-plan.pdf

Smith, C. L., & Brooks, D. J. (2013). *Security science : the theory and practice of security*. Butterworth-Heinemann.

Socialist Republic of Viet Nam. (2021). *National Green Growth Strategy for 2021-2030, vision towards 2050* https://en.baochinhphu.vn/national-green-growth-strategy-for-2021-2030-vision-towards-2050-11142515.htm

Sørskår, L. I. K., Abrahamsen, E. B., & Abrahamsen, H. B. (2017). On the use of economic analyses when evaluating new technology in helicopter emergency medical services. *I: Safety & Reliability, Theory and Applications*, 153-160.

Sørskår, L. I. K., Abrahamsen, E. B., & Abrahamsen, H. B. (2019). On the use of economic evaluation of new technology in helicopter emergency medical services *International Journal of Business Continuity and Risk Management*. https://doi.org/10.1504/IJBCRM.2019.096693

The Governance Group AS. (2021). *Aker Solutions – Climate Risk Report*. The Governance Group AS. https://www.akersolutions.com/globalassets/sustainability/tcfd-climate-risk-review-2021.pdf

The Government of Japan. (2022). *Clean Energy Strategy to Achieve Carbon Neutrality by 2050*. The Government of Japan. Retrieved from https://www.japan.go.jp/kizuna/_userdata/pdf/2022/summer2022_special_issue/clean_energy_strategy.pdf

The International Partners Group. (2022a). *International Agreement to support Viet Nam's ambitious climate and energy goals* https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_22_7671/IP_22_7671_EN.pdf

The International Partners Group. (2022b). *Joint Statement: South Africa Just Energy Transition Investment Plan* https://ec.europa.eu/commission/presscorner/api/files/document/print/en/statement_22_6664/STATEMENT_22_6664_EN.pdf

The Presidency Republic of South Africa. (2023). *South Africa's Just Energy Transition Investment Plan (JET IP)*. The Presidency Republic of South Africa. Retrieved from https://www.thepresidency.gov.za/download/file/fid/2649

U.S. Department of Energy. (2021). *WETO Lasting Impressions 2021*. (DOE/GO-102021-5842). U.S. Department of Energy. Retrieved from https://www.energy.gov/eere/wind/articles/wind-energy-technologies-office-lasting-impressions

UK Department for Business Energy & Industrial Strategy, & Skidmore, C. (2019). *UK becomes first major economy to pass net zero emissions law* https://www.gov.uk/government/news/uk-becomes-first-major-economy-to-pass-net-zero-emissions-law

UK Government. (2018). *Overseas business risk: Colombia*. UK Government. https://www.gov.uk/government/publications/overseas-business-risk-colombia/overseas-business-risk-colombia

UK Government. (2021a). *Overseas business risk: Chile*. UK Government. https://www.gov.uk/government/publications/overseas-business-risk-chile/overseas-business-risk-chile

UK Government. (2021b). *Overseas business risk: Vietnam*. UK Government. https://www.gov.uk/government/publications/overseas-business-risk-vietnam/overseas-business-risk-vietnam#intellectual-property

USAID. (2022). *Colombia Climate Change Fact Sheet* USAID. Retrieved from https://www.usaid.gov/sites/default/files/2023-03/2022-USAID-Colombia-Climate-Change-Country-Profile.pdf