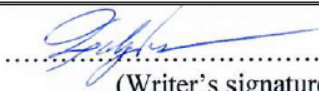




University of  
Stavanger

Faculty of Science and Technology

## MASTER'S THESIS

Study program/Specialization: MSc in Risk Analysis and Governance	Spring semester, 2021  Open / Restricted access
Writer: Evangelia Trivyadaki	 ..... (Writer's signature)
Faculty supervisor: Roger Flage  External supervisor(s):	
Thesis title:  Assessing home office cyber risks in the oil and gas industry A comparative study of risk assessment methods	
Credits (ECTS): 30	
Key words: risk assessment, risk analysis, home office, oil and gas, covid-19, information security, cyber security, cyber threat, IRAM2, ISO 27005:2018, Octave Allegro, NIST SP800-30, FAIR	Pages: 72  + enclosure: 2  Stavanger, 15 / 06 / 2021 Date/year

# Assessing home office cyber risks in the oil & gas industry

A comparative study of risk assessment methods

## Abstract

Home Office has become a necessity nowadays, as it is part of the business continuity plan for many companies and organizations worldwide, ever since the COVID-19 outbreak made its presence in 2020. Even though it is not new as a concept, it has had a rapid growth, and it is now heavily used even within business areas that preferred to have all employees working from corporate offices. The oil and gas industry is such an example, since companies with a presence in that area, would always prefer to have their employees on-site, rather than working remotely. The aggressive introduction of “Work from Home” solutions though, comes with significant cyber risks that are not to be taken lightly.

The aim of this thesis is to analyze a set of common risk assessment methodologies that are used in information security and test their effectiveness in terms of assessing cybersecurity risks related to the home office implementation in the oil and gas industry. The methodologies under investigation are IRAM<sub>2</sub>, ISO 27005:2018, Octave Allegro, FAIR and NIST SP800-30. According to the findings, there are specific strengths and limitations that risk analysts, decision-makers and other relevant stakeholders need to consider while using one or more of these methods for this specific use-case. The most important factor is time, which causes significant impediments for all involved parties and limits the options that can be considered, for reacting to the rationality of the situation. There are also more generic learnings though which are applicable even if companies had more time for properly assessing cyber risks before introducing remote worker solutions. The outcome of the research leans towards the use of two or more different risk assessment methodologies, which can be combined depending on the company’s needs and the project in scope. The learnings of this thesis can be useful for future potential incidents of a similar nature.

## Acknowledgement

Perhaps one of most famous quotes to be found in Steve Jobs' biography, is "*Great things in business are never done by one person; they're done by a team of people*" (BusinessNewsDaily, 2019). I strongly believe that this quote perfectly reflects the work and effort done for developing this thesis.

First, I would like to express my gratitude to my supervisor, Professor Roger Flage. His invaluable guidance, knowledge-sharing and his immediate and precise feedback have been of the outmost importance throughout this period. For this, I am forever grateful.

Moreover, I would also like to offer my sincere thanks and appreciation to Equinor ASA's cybersecurity risk analysts and operational experts, as well as IT managers and leaders who were kind enough to provide an interview with vital information for supporting this thesis with real examples.

Last, but certainly not least, I would like to thank my husband who always stood patiently by my side, and my two lovely kids for their encouragement with lots of hugs.

## Table of Contents

Abstract.....	iii
Acknowledgement .....	iv
1. Introduction .....	1
1.1. Background .....	1
1.2. Main objectives & research questions.....	2
1.3. Limitations and considerations.....	2
1.4. Thesis structure .....	3
2. Theory.....	4
2.1. Risk concept, risk description & vulnerability.....	4
2.2. Risk management .....	5
2.3. Risk analysis.....	6
2.4. The risk assessment process.....	7
2.5. Information security & cyber security fundamentals.....	9
2.5.1. Information security.....	9
2.5.2. Cyber security .....	11
2.5.3. Cyber security threats & vulnerabilities .....	12
3. Context description.....	16
3.1. Common “Home Office” cyber security risks .....	16
3.1.1. Phishing emails .....	16
3.1.2. Bring Your Own Device (BYOD).....	17
3.1.3. Home network security .....	18
3.2. Oil & gas industry information .....	19
3.2.1. Industry description .....	19
3.2.2. Oil & gas IT infrastructure & cyber security unique characteristics .....	19
3.3. Past oil & gas industry cyber security incidents .....	20
3.3.1. Norsk Hydro.....	20
3.3.2. Pemex.....	21
3.3.3. Saudi Aramco.....	21
3.4. Oil & gas industry “Home Office” cyber security risks.....	22
4. Research methodology .....	23
4.1. Literature review .....	23
4.2. Interview.....	24
4.3. Linking research methodologies to research questions.....	25

5.	Information security risk assessments .....	26
5.1.	Introducing information security risk assessments .....	26
5.2.	Selecting common information security risk assessments .....	26
5.3.	Information security risk assessment methodologies analysis .....	27
5.3.1.	IRAM <sub>2</sub> .....	27
5.3.2.	ISO/IEC - ISO 27005:2018.....	29
5.3.3.	Octave Allegro .....	32
5.3.4.	FAIR .....	33
5.3.5.	NIST SP800-30.....	36
6.	Equinor ASA case study .....	39
6.1.	Pre-“Home Office” implementation interview feedback .....	39
6.2.	Post-“Home Office” implementation interview feedback .....	40
6.3.	Oil & gas industry cyber security interview feedback .....	41
6.4.	Risk assessment methodologies interview feedback.....	41
7.	Risk assessments effectiveness on home office from an oil & gas industry perspective .....	43
7.1.	Basics of evaluating risk assessment quality.....	43
7.2.	Risk assessments review .....	44
7.2.1.	The time factor consideration .....	44
7.2.2.	Risk assessment methodologies evaluation .....	45
8.	Discussion.....	51
8.1.	Findings.....	51
8.2.	Suggestions.....	53
8.3.	Future research .....	56
9.	Conclusions .....	57
	Bibliography .....	58
	Appendix.....	67
	Appendix I – Interview questionnaire.....	67
	Questions on the risk assessment methodologies .....	67
	Questions on risk assessments, emergency plans and/or business continuity plans, related to COVID-19 “Home Office” and cyber security .....	67
	Questions related to the “Home Office” situation .....	67
	Questions related to cyber security in the oil and gas industry .....	68

# 1. Introduction

## 1.1. Background

It is beyond doubt that the event that scarved its dominant mark more than any other in the year 2020, is the COVID-19 pandemic. It all started in Wuhan China, where the first cases were reported and identified as “viral pneumonia”. Two weeks later, the first epidemiological alert was raised by PAHO/AMRO and a few days later, it was first announced that human-to-human transmission is possible (WHO, 2020). Officially, the virus appeared in Europe, France on the 24<sup>th</sup> of January 2020, however latter reports indicate that the first case was a patient that was treated in the same country on the 27<sup>th</sup> of December in 2019 (BBC, 2020). The virus quickly spread across the continent, and it also started having a vivid presence in the American continent as well. The results have been devastating so far in many different aspects. From a humanitarian perspective, 110 million of cases have been identified, and almost 2.5 million deaths have been reported until mid-February 2021 (WHO, 2021). The impact on global economy is equally overwhelming, mainly due to the global trading collapse (WTO, 2020), the rise of unemployment (Tennant, 2020) and the investments hesitance (Jackson, et al., 2020, p. 30).

As a response to the outbreak, many governments worldwide took urgent measures in an effort to limit the virus spread, and to support their health system. One of the measures that was introduced globally, was to shut down most public and private sector business for a period of time, so that people can remain isolated at home, hence drastically reducing the chances of having infected people transmitting the virus to healthy ones. This measure though had a significant impact on private sector companies / organizations, since they could no longer operate properly which resulted in heavy financial losses.

As a proactive (and in certain cases as a reactive) measure, many companies, regardless of their size, started looking into options that could potentially ensure business continuity to a large scale through the pandemic. The most popular of those measures, was to introduce “Home Office” as a method for having their employees working remotely from home by using digital means such as a company-provided or personal PC / laptop. Even though home office is not new as a concept, it has never been used in such a large scale.

Naturally though, the “Home Office” approach is not suitable for all business sectors. For example, quite often, the nature of the work requires the physical presence of an employee in the company premises. Another example is a company being hesitant to expose digital services on the internet for facilitating remote employees, due to the fear of having those services and the information they expose, compromised by malicious users. Both of those two used cases are applicable to the oil & gas industry, which traditionally prefers having employees in-house doing the required tasks. Due to the pandemic though, the industry was forced to adapt to the new standards, and digital remote workers have now become a reality for many oil & gas organizations.

The decision making, as well as the transition period and methods, were not the same for all companies. Some of them might have chosen to pro-actively test scenarios where they would have to close their offices and have most of their employees working remotely, due to a number of potential root causes they may have thought. Other organizations might have considered home office in a much smaller scale, and some other may have not even thought of the possibility of such a scenario. It is safe to assume though that most (if not all) oil & gas companies that enabled WFH (Work from Home) methods, must have done research and evaluation on the related risks, the chances of them occurring and their potential impact.

## 1.2. Main objectives & research questions

The purpose of this thesis is to evaluate a set of common cyber security risk assessment methods in relation to the “Home Office” situation that has emerged ever since the COVID-19 outbreak. The focus of the thesis will be the oil & gas sector, and the challenges it faces due to its unique characteristics. The end goal is to provide suggestions to risk analysts and decision-makers within the industry, on how to approach similar use-cases in the future. The suggestions and findings are based on risk science data and the conducted analysis. The following research questions need to be addressed as basis before providing suggestions / recommendations:

1. What are the most common / widely used risk assessment methods related to cyber security risks, and what are their main characteristics?
2. What are the advantages and disadvantages of each of those risk assessment methods from a risk science point of view?
3. How effective is each risk assessment method for evaluating the risks of the “Work from Home” situation in the oil & gas industry, in both planned and unplanned (such as the COVID-19 use-case) scenarios?

## 1.3. Limitations and considerations

Prior to conducting the scientific analysis of this thesis, certain limitations must be highlighted. The conducted analysis is focused on the home office cyber security risks only. This does not mean that the only risks related to working from home are originating from the cyber threats landscape. Certain other risks that come into the picture, can be the physical and mental health of the employee.

Another limitation is in relevance to identifying the most common risk assessment methodologies in today’s industry. For the scope of this thesis, five have been selected, based on literature review, as well as data gathered from the interview.

Moreover, the result of this research also depends on quality of the data that is to be gathered from Equinor ASA, and more specifically from the company’s cyber security and risk management experts’ input. The interview information is used as support case study for providing a real-world example from the industry, however other



organizations in the business sector might have dealt with the home office situation in a different way. Furthermore, it should be stated that the author has relatively limited knowledge on information security science.

An important consideration is the partial usage and reflection of the author's personal judgement, while comparing risk assessment methodologies and producing findings and suggestions. This comes as a logical inference and it is heavily based on the analysis and review of relevant literature and interview data presented in this thesis.

#### 1.4. Thesis structure

The first part of the thesis is dedicated to establishing a theoretical framework. More specifically, it provides a basic analysis on the risk concept and its description, as well as on risk management / risk analysis fundamentals, and the risk assessment process.

As a follow up, a detailed background section establishes a clear understanding of certain elements, such as a short oil & gas business sector description, the unique characteristics of that business area in relation to remote workforce, past use-cases that provide insight on remote digital workers in the industry, and the most common cyber threats that emerge for energy organizations using "Work from Home" techniques for ensuring business continuity during the pandemic.

The next chapter is focused on the research methodology. It provides details on the methods that have been chosen, as well as arguments for supporting these choices.

Moving to the next chapter, the research shifts focus on cyber security risk assessment methods. More specifically, it provides a list of the most common cyber security risk assessment types, utilized in the oil & gas industry, as well as an overview of their characteristics, and an analysis of advantages and disadvantages associated with each of the listed methods.

A support case study from Equinor ASA, a major oil & gas company, follows, providing information and real data on how an enterprise-level organization dealt implemented home office solutions for its employees, and how it dealt with the "Work from Home" risks.

The data presented in the theory and context sections, as well as the risk assessment methodologies presentation and the case study, are used as a basis to conduct a review for strengths and limitations for the pre-selected risk assessment methodologies, in the scenario of using them for analyzing risks related to working from home solutions, from an oil & gas industry perspective.

The final part of the thesis is devoted to discussions on the research evaluations, as well as on the scientific findings. It also provides recommendations and suggestions to the risk analysis experts, as well as future research proposals that could evolve and/or enhance the research even further.

## 2. Theory

The theory presented in this chapter is the basis of understanding the core content and the scientific breakdown of the thesis. More specifically, the first subchapter provides an analysis on “risk concept” fundamentals, as well as the “risk description” of the scientific term. Furthermore, it contains a basic explanation of “vulnerability”, a term widely used in risk science. The following subchapter contains a discussion on risk management, risk analysis and risk assessment methods, while the last one provides a generic analysis on cyber security basics.

### 2.1. Risk concept, risk description & vulnerability

Over the past few decades, many efforts have been made to establish a specific definition on risk that is both understandable and acceptable from the global scientific community. To address this challenge, the Society of Risk Analysis (SRA) has introduced an authoritative glossary of risk, which consists of seven qualitative definitions (Aven, 2020, p. 58). According to them, risk is:

- *the possibility of an unfortunate occurrence.*
- *the potential for realization of unwanted, negative consequences of an event.*
- *exposure to a proposition (e.g. the occurrence of a loss) of which one is uncertain.*
- *the consequences of the activity and associated uncertainties.*
- *uncertainty about and severity of the consequences of an activity with respect to something that humans value.*
- *the occurrences of some specified consequences of the activity and associated uncertainties.*
- *the deviation from a reference value and associated uncertainties.*

Aven’s approach is aligned with SRA’s definitions. According to him, the risk concept consists of two main features, Consequences (C) and Uncertainty (U). The former refers to something that humans value, while the latter refers to the uncertainty (possibility/potential). More specifically, the risk (A, C, U) of an event (A) will lead to consequences (C), which are characterized by uncertainties (U), since no one is fully aware of what will occur in the future (Aven, 2020, p. 58).

This definition can be further elaborated by using home office in the oil and gas industry as an example. The activity considered in this thesis is “Work from Home” for oil and gas companies. risk analysts, decision-makers, and other relevant stakeholders need to investigate the potential consequences of this activity in terms of cyber security events (A) and their potential consequences/impact (C). There is uncertainty (U) characterizing both (A) and (C), which implies to a condition of risk, where risk is understood as (A, C, U).

In order to be able to manage risk, it is important to have the ability to describe it and/or to measure it. According to Aven, the risk description can be expressed by the following concept:

$$\text{Risk description} = (C', Q, K)$$

where (C') are the specified consequences, (Q) is the measurement of uncertainty (typically measured using probability (P)), and (K) is the background knowledge on which (C') and (Q) are based on. Another way of describing risk is (A', C', Q', K), where A' references specified undesirable events (Aven, 2020, pp. 60-62).

Moreover, Aven inaugurates “Vulnerability” into the risk concept fundamentals. Vulnerability, is the risk conditional on the occurrence of an event (A), and it is described as the combination of consequences and the associated uncertainty given an event (Aven, 2015, p. 19). By using the appropriate symbols, the risk can be defined as: threats, uncertainties (A, U) + vulnerability (C', U | A). Thus, vulnerability description is the following: (C', Q, K | A) (Aven, 2015, p. 19).

## 2.2. Risk management

Nowadays, it is widely accepted from the global market that exploitation of new opportunities imposes risks, since it is something that cannot be eliminated. Therefore, modern organizations and business sectors in general, choose to manage risk instead. risk management as a definition, contains all of the activities required with the purpose to manage risk (Aven & Vinnem, 2007, p. 1). Aven states that risk management is about balancing development and exploring opportunities on one hand, and protection avoiding losses, disasters and accidents on the other (Aven & Vinnem, 2007, p. 2). SRA offers a similar terminology, since it defines it as the activities to handle risk such as prevention, mitigation, adaptation or sharing (SRA, 2018). According to SRA, risk management also includes potential compromises between cost and benefit of risk deductions, as well as the option of accepting some risks as tolerable. ISO 31000 describes it as a set of coordinated activities that aim to direct and control an organization in terms of risk (ISO 31000:2018, 2018).

Aven claims that most organizations worldwide choose to divide risk management into three categories, strategic, financial and operational (Aven, 2015, pp. 4-5).

1. The strategic risk refers to risks where the consequences are mainly originating from mergers, acquisitions, laws and/or regulations, labor market, technology, competition and political conditions.
2. The financial risk alludes to risks where the consequences are related to the global market. Potential factors (amongst others) could be stock prices, interest rates, foreign exchange rates, or commodity prices.
3. The operational risk denotes risks where the consequences are a result of safety and/or security related issues, such as accidental events or intentional acts.

The risk management process involves many steps / phases. According to ISO 31000:2018, it includes establishing the scope, context and criteria, the risk assessment phase which includes risk identification, risk analysis and evaluation, the risk treatment phase, communication and consultation, monitoring and review, as well as recording and reporting. Risk analysis is considered to be the central part of this process (ISO 31000:2018, 2018).

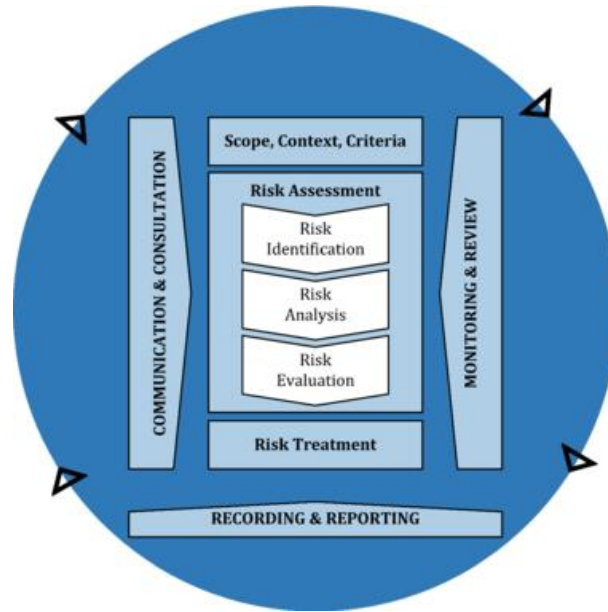


Figure 1 – ISO 31000:2018 Risk Management Process

### 2.3. Risk analysis

Risk analysis aims to describe risk and to present an informative risk picture with the use of different methods (Aven, 2015, p. 1). There are three main categories of risk analysis methods depending on their simplicity and complexity, and two different types, qualitative or quantitative. The following table provides an overview of the risk analysis categories, as well as a core description for each (Aven, 2015, p. 2):

Main Category	Type of Analysis	Description
<b>Simplified risk analysis</b>	Qualitative	Simplified risk analysis is an informal procedure mainly utilizing brainstorming sessions and group discussions for establishing the risk picture. Risk is usually classified on a coarse scale.
<b>Standard risk analysis</b>	Qualitative or quantitative	Standard risk analysis is a more formalized procedure compared to the simplified one, since it utilizes risk analysis methods such as Hazard and Operability study (HAZOP) or coarse risk analysis. Risk matrices are often used to present results.
<b>Model-based risk analysis</b>	Primarily quantitative	Model-based risk analysis utilizes more complex, quantitative techniques to calculate risk.

Table 1 – Main Categories of risk analysis methods

According to Aven, there are multiple risk analysis models, however the most common structure contains three main phases, which are “Planning”, “Risk Assessment (execution)”, and “Risk Treatment (use)” (Aven, 2015, p. 5). The planning phase includes problem definition, information gathering, organizing the whole work and selection of the risk method. The risk assessment is the main part of the risk analysis which aims to identify the initiating events (threats, hazards, opportunities), and to conduct a cause and consequence analysis in order to establish a risk picture. The next phase is the comparison of all alternatives, as well as identification and assessment of measures. The last part is the management review and judgement with the final goal to make decisions for the risk treatment. The following figure provides a high overview of risk analysis (Aven, 2015, p. 6):

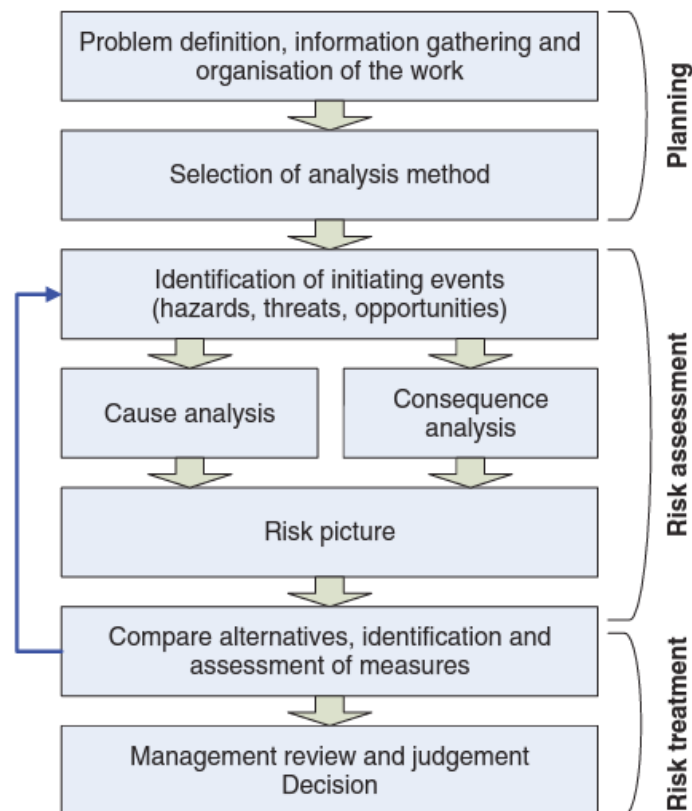


Figure 2 – Risk Analysis Process Overview

#### 2.4. The risk assessment process

According to Aven, the risk assessment process is one of the core components of risk analysis (Figure 2). He defines risk assessment as the systematic process during which risk sources, threats, hazards and opportunities are discovered. Moreover, during this process, the relevant involved parties can obtain a better understanding of how such events can occur and what are the potential consequences. It is also used as a mean for risk and uncertainties expression and representation, as well as for highlighting the gravity of each of the identified risks by using relevant criteria (Aven, 2020, p. 87). According to the ISO 31000:2018 risk management process (Figure 1, p.9), the risk

assessment phase relates the above steps through risk identification, risk analysis and risk evaluation.

The first and most critical task of risk analysis is the identification of initiating events. The goal of this task is to identify risk sources, threats, hazards and opportunities that potentially may occur. It is of the outmost importance to execute it efficiently, since involved parties will not have the ability to reduce consequences of events that have not been identified. Therefore, this step needs to be carried out in a structured and systematic manner with the involvement of competent resources. During this task, various and suitable methods for each project can be used such as: FMEA (Failure modes and effects analysis), HAZOP (Hazard and operability study), SWIFT (Structured what-if technique). All these methods are based on structured brainstorming, during which experts use means such as checklists and guidewords (Aven, 2015, p. 38).

Cause Analysis follows as an equally critical task, during which experts are searching for the causes (the causal factors) that will lead to the occurrence of a pre-identified event. For the purpose of the cause analysis task, the involved parties are using different methods and techniques such as brainstorming, event tree analysis or Bayesian networks. In order to achieve a solid result, it is mandatory to thoroughly examine the system knowledge. Moreover, in addition to the main cause analysis, some sub-risk analysis tasks may follow for each of the risks found (Aven, 2015, pp. 39-40).

The consequence analysis utilization targets the discovery of possible consequences for every initiating event. The most common methods used are Event tree analysis (ETA) and Fault tree analysis (FTA).

The combination from the cause and consequence analysis provides insights in order to establish the risk picture. According to Aven, this picture covers the risk description ( $A'$ ,  $C'$ ,  $Q'$ ,  $K$ ), where ( $Q'$ ) refers to probabilities ( $P$ ) and SoK (strength of knowledge assessment). The risk picture should cover the following aspects:

- Predictions of the quantities the experts are interested in (e.g. number of fatalities, costs)
- Probability distributions (e.g. related to costs and number of fatalities)
- Strength of knowledge
- Manageability factors

One simple and understandable way to present the risk picture is the use of risk matrices (table 2). They present risk based on probabilities and consequences. Risk science experts should be aware though that the use of this tool has some limitations. Therefore, both dimensions should be followed by the background knowledge ( $K$ ), and more specifically by the strength of this knowledge (SoK), which in turn can be judged as weak or strong depending on special circumstances (Aven, 2020, p. 129). The value of the strength of knowledge is considered to have an important role in risk picture and consequently in supporting decision makers for a better evaluation and treatment of the risk.

		Likelihood				
Consequences		Rare (1)	Remote (2)	Occasional (3)	Frequent (4)	Almost Certain (5)
	Catastrophic (5)	5	10	15	20	25
	Major (4)	4	8	12	16	20
	Moderate (3)	3	6	9	12	15
	Minor (2)	2	4	6	8	10
	Negligible (1)	1	2	3	4	5

Table 2 – A typical 5x5 risk matrix example (O' Reilly, n.d.)

## 2.5. Information security & cyber security fundamentals

### 2.5.1. Information security

A key objective of the thesis is to investigate the effectiveness of common risk assessment methods on evaluating cyber risks related to home office for the oil & gas industry. It is therefore important to provide a good understanding of what information security and cyber security are, since those two terms are very often mistakenly conceived as one. According to the Committee on National Security Systems (CNSS), *“Information security is the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information”* (Whitmain & Mattord, 2011, p. 8). It includes information security management, computer and data security, and network security. Information security is related to both physical and digital forms of data.

Information security management refers to controls that are implemented by an organization, in order to protect the confidentiality, integrity and availability of its data. The three latter are also widely known as the “C.I.A.” triangle.

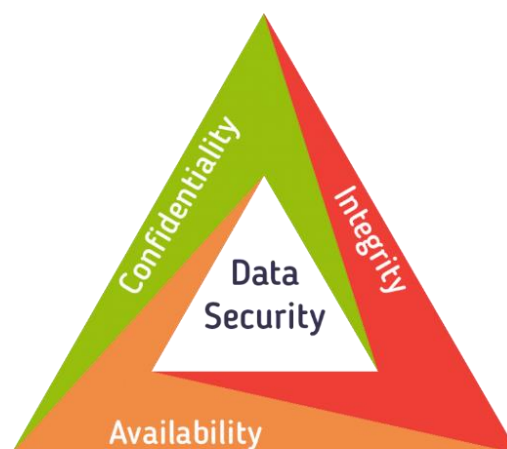


Figure 3 – C.I.A. Triangle / Triad (Devopedia, n.d.)

**Confidentiality** is important because it ensures that the information in scope is only available to a set of individuals or systems that should have the authorization to access it. In other words, Confidentiality prevents unauthorized access to the information in question. The following example highlights its importance, as well as its potential consequences: An organizational document contains information on a scientific discovery that can give the company an advantage against its competition. A certain individual manages to bypass authorization techniques, get a copy of the documents, and sell it to competition. Confidentiality is breached, and the result is financial loss for the organization that suffered the incident. Another important aspect is controlling access on information related to employees, as well as customers who interact with the company / organization. Many governments worldwide are forcing organizations and companies to follow specific guidelines and protocols for ensuring confidentiality of personal data. The European Union for example, has implemented the widely known “General Data Protection Regulation” (also known as G.D.P.R.), which is the strongest data privacy and security law worldwide (EU, n.d.). The most common techniques used for ensuring confidentiality are information classification, secure document storage, application of general security policies, and education of information custodians and end users (Whitmain & Mattord, 2011, p. 13). For example, many organizations choose to classify their digital documents / information with relevant labels, such as “Public”, “Internal”, “Restricted” or “Confidential”. This classification follows principles set in ISO 27001 and it defines who should have access on the pre-classified digital information (Calder & Watkins, 2015, pp. 127-129).

**Integrity** is an equally important information security pylon. Information has integrity, when it is certain that it is whole, complete and uncorrupted or unaltered. If a hacker manages to obtain access to sensitive data, it is possible to modify it or delete it, which could cause a series of reactions. The following example illustrates and provides a better understanding of the importance of integrity: A company uses digital means for paying their suppliers. A hacker manages to gain access to their centralized payment system where suppliers records are kept, and modifies their bank accounts to international ones, owned by him/her. The company will suffer financial damage since they will be liable to their suppliers and it will be challenging to trace the illegal payments for obtaining their funds back. Hackers are not the only threat against a potential data corruption. Whitmain mentions other examples as well, such as corruption of data during transmission (Whitmain & Mattord, 2011, p. 15).

The last pylon of the CIA triangle is **Availability**. Authorized users and systems must have the ability to access the information they seek at all times. The following scenario can provide a better understanding of availability: A retail store uses an e-commerce platform for selling goods to customers. The platform is hosted on a network secured zone, meaning that there are information security mechanisms /technologies in front of it, for protecting it against malicious users, and for authenticating customers, as well as administrators that operate it and maintain it. If the information security technologies malfunction, the e-commerce package is no longer available towards its users, therefore the company has a negative financial impact. It is therefore important to ensure the best possible uptime.



Certain IT security experts tend to expand the classic CIA triangle even further. For example, P.W. Singer and Allan Friedman highlight the importance of one more aspect, which is **Resilience** (Singer & Friedman, 2014, p. 35). They describe resilience as a key mechanism that safeguards endurance of a system while it faces security threats, and therefore prevents a potential system failure. The authors accept the realistic assumption that cyber-attacks and/or security incidents can and will eventually happen, therefore it is important to ensure that the affected system will continue serving its purpose, unaffected from threats.

### 2.5.2. Cyber security

Cyber security is a part / subset of information security. Usually, the term “Cyber Security” refers to the technical means being used for protecting the digital forms of data within a company or an organization from threats or vulnerabilities. This comes in contrast to “information security”, where the scope is to protect any forms of data, digital or even physical. In the modern IT era, most of the information / data within an organization, has a digital form, therefore cyber security is a major part of information security. The following figure from Dejan Kosutic, reflects the relationship between Risk Management, Information Security, Cyber Security, Business Continuity and Information Technology (Kosutic, 2016):

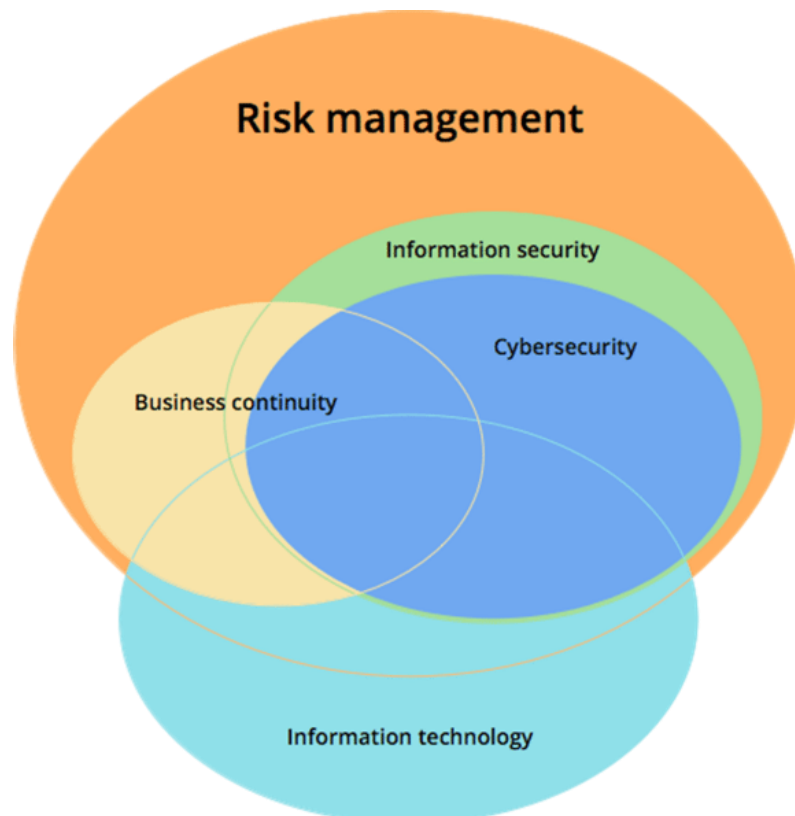


Figure 4 – Relationship between Risk Management, Information Security, Cyber Security, Business Continuity and Information Technology (Kosutic, 2016).

### 2.5.3. Cyber security threats & vulnerabilities

People often mix and/or misunderstand threats and vulnerabilities related to cyber security, and they often perceive them as one, which is not a valid fact. According to the Committee on National Security Systems (CNSS), a threat is defined as “Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service” (CNSS, 2015, p. 122). In a more generic approach, cyber threats are malicious acts that aim towards a partial or total compromise of one or more information systems. The end-goal of the attacker is to negatively affect aspects related to the CIA triad. There are many types of cyber threat actors, and they are often driven by different motivations, depending on their origin, motivation, as well as their target. For example, certain nations / countries tend to attack other ones, hence motivation is mostly driven by geopolitical factors. Cybercriminals are mostly focused on profit, and terrorists from ideological violence. The following figure from the Canadian Centre for Cyber Security, presents an overview of the most common cyber threat actors, as well as the motivation behind their actions (Canadian Centre For Cyber Security, 2020, p. 2):

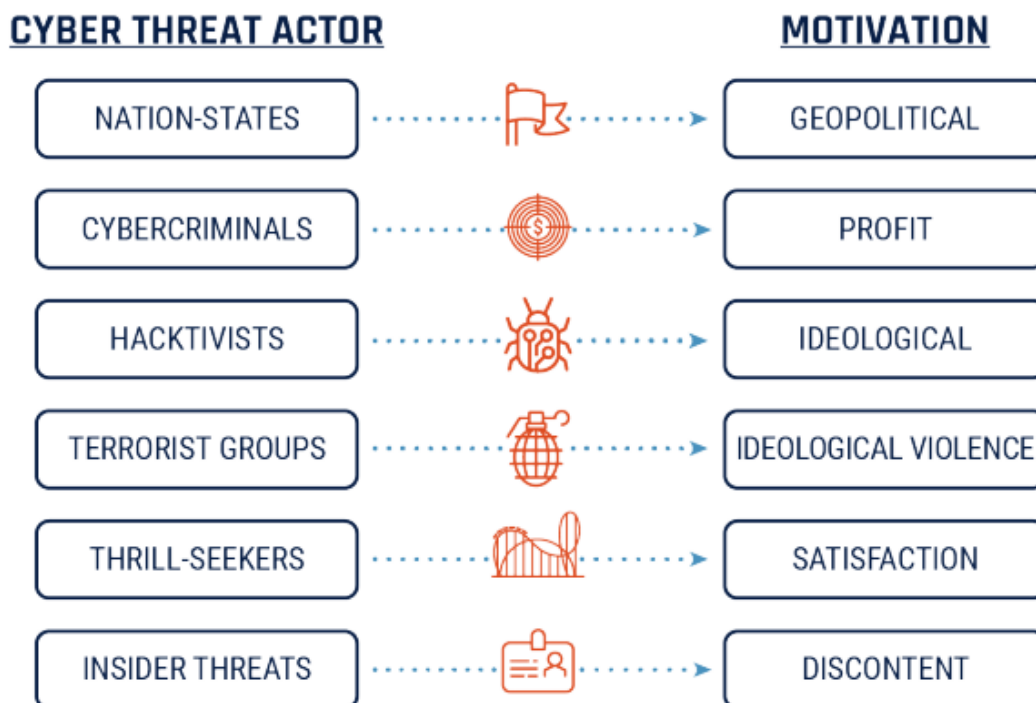


Figure 5 – Cyber Threat Actors and their motives according to the Canadian Centre for Cyber Security

The cyber threat landscape is something dynamic since new threats constantly emerge, while some others tend to fade in time and re-surface depending on various circumstances. The most common ones nowadays are the following:

- **Social Engineering.** Perhaps the most common cyber attack nowadays, is social engineering. The term refers to manipulation techniques used from attackers, in order to exploit human errors. The end goal is to lead individuals or groups of individuals towards personal data exposure such as usernames/passwords, or even gaining access to personal systems. A classic example is an attacker calling the potential victim after gathering personal information through various sources (e.g. social media such as Facebook), imitating to be someone from the victim's bank. The attacker often tries to convince the user that his/her personal account has been compromised, and hence personal information is required for verifying the victim's identity and for securing the account again. The panicked victim often shares username/password to the attacker; hence the bank account credentials are compromised. Another example of social engineering attacks is the "Phishing Attack". The malicious user implements a sophisticated email which appears to be coming from a familiar source to the victim (employer, bank, etc.). The email contains links, trying to lure him/her into clicking one of them. If the victim clicks, a web site opens which appears to be from the familiar source, e.g. the victim's bank. When the user attempts to logon, his/her credentials are stolen from the attacker. According to Verizon (one of the largest WAN / Internet providers worldwide), social engineering was the technique responsible for more than one third of the total breaches that took place in 2020 (Verizon, 2020, p. 13).
- **Ransomware.** Ransomware refers to malicious software that upon its deployment in a victim's system, it targets and encrypts personal files and folders, making them completely inaccessible. Once encryption is done, the software pops up a message asking the user to do a one-time ransom payment to the attacker within a certain amount of time, which is usually 48 – 72 hours. If the victim pays the ransom, the attacker shares the decryption password and the victim is able to obtain access to the files again. The ransom is usually paid with cryptocurrency, since it is nearly impossible for the authorities to trace the payment back to the attacker. Ransomware was the third most popular cyber threat in 2020 since it was responsible for more than 20% of the total amount of breaches during that year (Verizon, 2020, p. 13).
- **Denial of Service (DDoS).** The Denial of Service attack mainly aims the "Availability" part of the CIA triad. Hackers deploy a massive number of clients that they either own, or they have compromised, in order to create many requests towards an internet exposed service. The end goal is to flood this service / server with requests and make it impossible for clients / customers accessing that service to get the information they want. An example could be a government internet exposed service that serves public health. The website is designed to accept a maximum of 2.000 simultaneous requests. If attackers perform a DDoS attack, sending more than 5.000 requests per second, the service will be unable to serve the content to valid civilians, and it will eventually crash due to lack of resources. According to Help Net Security, more than 4.83 million DDoS

attacks occurred during the first half of 2020, which was a 15% increase compared to H2 2019 (HelpNetSecurity, 2020).

- **Crypto Jacking.** Crypto jacking refers to malicious crypto mining software deployed from the attacker in the victim's system. The end goal is to utilize the hardware resources from the victim's computer for solving complex mathematical algorithms, which then lead to crypto coins generation (e.g., bitcoin). Crypto jacking is hard to detect since the victim is often unable to realize that system resources are over-utilized. The popularity of this attack often depends on the crypto coin prices. If the crypto coin market is down, crypto jacking is less popular and attackers tend to use other techniques for gaining money, such as ransomware.
- **SQL Injection Attacks.** SQL injection is a rather old, but still popular cyber threat. Many web services rely on SQL databases on the backend, either for verifying user credentials, or for providing data towards the clients. System owners / administrators might do a mistake leaving a database exposed to malicious SQL code. The attacker takes advantage of text input boxes / fields within the website, in order to send malicious code to the database. The result can be a completely loss of the database, or theft of data.

Vulnerabilities on the other hand refer to certain weaknesses that may exist within an IT technology / system which may be exploited from attackers. CNSS defines vulnerability as a "*Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source*" (CNSS, 2015, p. 131). Even though vulnerabilities are not the same as threats, there is an obvious connection between the two. An attacker may seek a vulnerability within the IT infrastructure of a company / organization, which can then be exploited to perform a cyber-attack. A few of the most common vulnerabilities nowadays are:

- **Zero-Day Exploits.** A zero-day exploit is a cyber-attack that is performed on the very same day that a vulnerability is discovered in a system. The vulnerability can be software or hardware related. The following example demonstrates a potential zero-day exploit. A large organization's IT infrastructure is heavily based on software that exposes a series of web services over the internet. A security organization discovers a weakness on that software, which can be exploited by attackers, allowing them to gain control over the environment. The software vendor is notified on the weakness and releases a critical security patch for mitigating the exposure. The organization though hesitates to deploy the patch because there is a requirement according to the organization's governing documents, to test patches on Quality Assurance systems prior to deploying them in production. An attacker who has the technical ability to exploit that weakness, attacks the company's web services and gains control of the environment. The potential impact can be catastrophic both from in technological and financial terms.
- **Software Bug.** Directly related to the above, a mistake on the programming code of software utilized by organizations, can also be catastrophic since in many cases, it is malicious users discovering such weaknesses in the software, rather than security companies or the software developers themselves.

- **Unencrypted Data.** If data travels within a company's network or over the internet without encryption, it is vulnerable to attacks related to data theft. The most common technique used from attackers in such cases is the "Man-In-The-Middle" attack, where the attacker intercepts the data in the network while it is transferred between two peers.
- **Elevated Account Privileges.** In most cases, for daily work, user accounts do not require elevated or administrator privileges. Certain users choose to have constant administrator privileges enabled, leaving their system vulnerable to attackers, since a potential credentials theft could allow the malicious user to have an absolute control over the affected system.

## 3. Context description

### 3.1. Common “Home Office” cyber security risks

Enterprise organizations worldwide traditionally tend to spend a significant amount of money for protecting their network perimeter, clients (laptops, workstations, mobile), as well as their IT services. The cyber security market grows constantly year by year, and it is expected to more than double in size until 2028, reaching an annual revenue of 366 billion USD (Fortune Business Insights, 2021).

As an outcome of the COVID-19 pandemic and the large scale of “Home Office” policies, many companies had to change their security infrastructure to be able to facilitate remote users. This required investments not just in cyber security, but on IT in general. Moreover, according to Gartner, companies that have implemented “Work from Home” solutions for their employees, intend to continue offering remote work as an option even after the pandemic is over, since 82% of them states that it will be allowed for employees to work remotely for some time, while 47% of them will allow full-time remote work (Gartner, 2020). From a cyber security perspective though, IT experts highlighted the fact that multiple risks were created and / or grew due to the large scale of remote working. This was expected, since large organizations that would not encourage remote work until now, would invest money on setting up strong network security perimeters for protecting services, clients and data. According to the CISO Benchmark Report of 2020 which was released just before the pandemic, securing mobile workers has been a great challenge even post-COVID-19, since 52% of the companies that participated in Cisco’s research responded that mobile device security is extremely difficult to deal with (Cisco, 2020, p. 14).

This section highlights the most common cyber security risks related to the global growth of the “Home Office” situation, which came as an aftermath of the COVID-19 virus outbreak (Cisco, 2020; Irwin, 2021; Kastner, 2021).

#### 3.1.1. Phishing emails

Phishing emails fall into the “Social Engineering” threat, and they aim on deceiving the victim to perceive them as genuine. They usually contain a link that leads the victim to fake websites which appear as real, or they contain a malicious attachment. The end goal is to either get the victim’s username and password since the victim might attempt to type credentials in the fake website, or to lead the affected user to download some type of malware (for example ransomware) or open an attachment which will compromise the user’s system. According to Infosecurity Magazine, phishing attacks, increased more than 600% in under a month, as soon as companies implemented remote work for their employees (Infosecurity Magazine, 2020). The source of information came from Barracuda Networks, a cyber security company specialized on threat intelligence. The security vendor reported that the phishing email incidents identified

were just 137 in January 2020, rising to 1188 in February and more than 9.000 in March. Most of the phishing emails had themes related to COVID-19, eventually tricking employees into clicking them since they thought they were genuine.

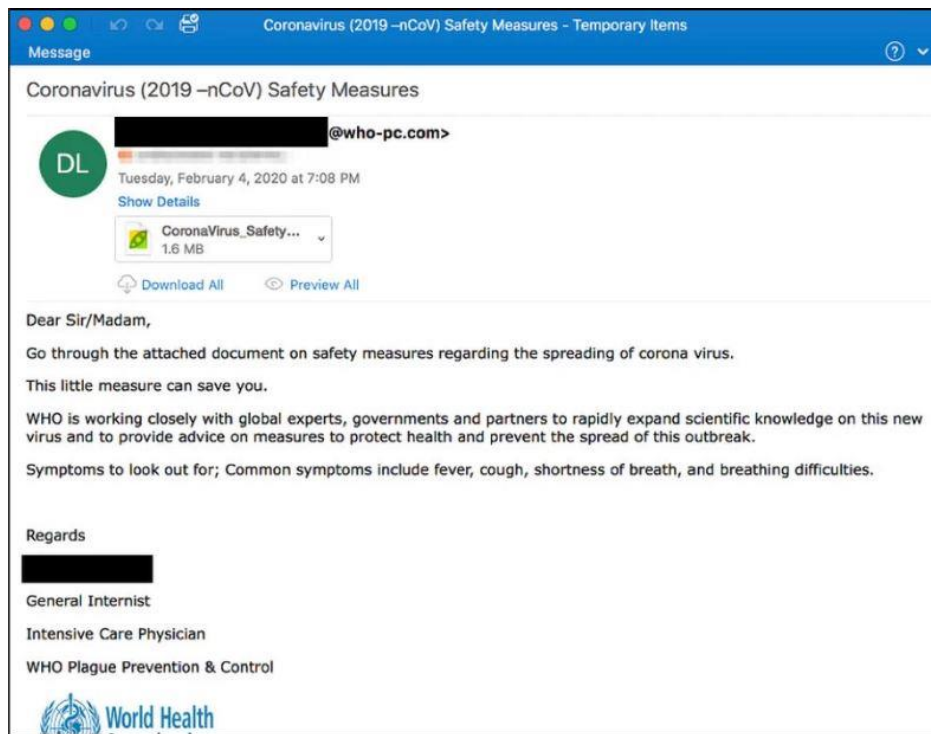


Figure 6 – Phishing Email that appears to originate from WHO (Kaspersky Labs, n.d.)

### 3.1.2. Bring Your Own Device (BYOD)

BYOD (Bring Your Own Device) refers to the strategy implemented by companies, allowing their employees to use their own personal devices (mobile phones, tables, laptops, workstations) for accessing company data and/or IT solutions (Gartner, n.d.). Since Q1 2020, when the Corona outbreak started, many organizations that shifted to a “Work from Home” policy, did not have sufficient resources to equip their employees with company-owned devices and/or it was something that would require a significant amount of time to do so. Therefore, they chose to deploy remote solutions that would allow their employees to use their own equipment, or they would fully or partially fund them to buy IT equipment and use it in a “Home Office” setup. BYOD market financial forecast reveal that the market will grow significantly over the next few years, due to organizations allowing remote work with personal devices (DigitalGuardian, 2020).

According to IT security experts though, BYOD has cyber security risks related to it, and large-scale BYOD policies can be a threat if not designed properly. As reported by a poll conducted by Outpost24 amongst 200 security partitioners, more than half of them reported that they have little or no visibility on the number of BYOD devices connecting into their company’s network and remote solutions (Outpost24, 2020). Other significant threats related to the use of personal devices for remote work, are weak passwords, users not encrypting the device storage, lack of backup policies,

inability for companies to have those devices wiped out remotely if needed (DigitalGuardian, 2020). Moreover, employee efficiency may be questioned since some organizations may choose to monitor the employee's activity, or to prevent them from accessing non-business-related web sites and applications. This is not technically possible on a BYOD device, because the employee owns the asset (TrendMicro, 2015). Another threat related to personal devices, is that in case of a potential device theft, company data may be stolen or lost.

In general, BYOD is not something organizations can apply strict policies on, because the device belongs to the employee. According to DigitalGuardian, 40% of large data breaches have been caused from BYOD, 50% of the companies that choose to allow the use of personal devices, have been breached via them and 60% of the organizations do not have the ability to delete company data from personal equipment that ex-employees used as a mean to work remotely (DigitalGuardian, 2020).

### 3.1.3. Home network security

A significant threat directly related to remote working is the potential compromise of the home network an employee is working from. Traditionally large organizations choose to heavily invest on cyber security defenses across their network perimeter, having their employees working securely inside the corporate network. A remote worker though does not have the same level of protection, because neither he/she or the company can afford to invest on cyber security equipment for protecting the home network.

Many organizations choose to use Virtual Private Network technologies for having their employees protected. VPNs are used for establishing a protected and encrypted network connection from a company owned laptop that is used in a home or public network, to the company's network, hence allowing the worker to perform tasks as if he/she is in the corporate network (Kaspersky Labs, n.d.). Companies, however, often allow the use of BYOD devices, and in some cases, even though an employee may have a company device, he/she may choose to use a personal one instead (DigitalGuardian, 2020).

Besides the threats that arise from the lack of security policies on a personal device, there is a bigger threat since the home network is not protected efficiently. A classic example related to Home Network security, is the potential compromise of another personal device that belongs to a family member, which can then be used as a mean to attach the device the employee is using for remote work. Internet of Things (IoT) is another similar major threat that needs to be considered. According to Gartner, IoT *“is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment”* (Gartner, n.d.). Many people choose to use IoT devices in their homes, effectively converting them to “smart homes” or “connected homes”. Smart home devices are utilizing the home network, as well as the internet, for offering a connected, real-time, smart home experience to the household inhabitants, since it allows them to control and monitor



their home remotely (Gartner, n.d.). Security focus has not been the main focus of IoT vendors though, especially for the first devices that were released in the market a few years ago. Consumers do not have the education or knowledge to properly configure IoT devices in terms of security, therefore they leave them exposed to hackers. A potential IoT device compromise could allow an attacker to use it as a mean to attack other devices inside the home network, including company or personal owned equipment that is used for remote working (TrendMicro, 2019).

## 3.2. Oil & gas industry information

### 3.2.1. Industry description

The oil & gas sector has traditionally been one of the world's largest. According to Fortune 500, it was the top sector worldwide in terms of revenue, and third in terms of profit in 2019 (GlobalData, 2019). Even though there is a major shift towards renewable energy worldwide, it is expected that the oil & gas industry will continue to grow, reaching a global production of 100 million barrels per day, mainly due to the increasing demand from the BRIC nations (Brazil, Russia, India and China) (Investopedia, 2020).

Structure-wise, the oil & gas industry is split into three segments, upstream, midstream and downstream. The upstream is also known as Exploration and Production (E&P), and it is focused on reservoirs discoveries and drilling of oil or gas wells. Midstream is responsible for transporting oil and gas from wells to refineries, while downstream is focused on refining tasks and the sale of the end-product (Investopedia, 2021). Some companies in the sector, choose to get involved only in certain segments, however there are others which are involved in all three, such as Royal Dutch Shell (Shell, n.d.).

### 3.2.2. Oil & gas IT infrastructure & cyber security unique characteristics

IT infrastructure and cyber security have some unique characteristics in the oil & gas industry, compared to other business sectors. Companies in the petroleum industry are extremely careful while designing and protecting what they call "Critical Infrastructure". Some IT systems are vital, not just for the survival of the company, but in certain cases, depending on the size of that company, they can be vital for a nation's economy as well. (Fortinet, n.d.).

In terms of upstream infrastructure, oil & gas have a complex IT infrastructure both onshore and offshore which can prove valuable targets for several types of hackers. Midstream is mostly related to the SCADA system (Supervisory Control and Data Acquisition) and the IoT devices being used for monitoring and control. A potential attack to the SCADA system that companies use for operating offshore rigs, wells, pipelines and refineries, can have a major impact on the environment, as well as operational disruptions, financial loss, reputational damage, and employee injury or loss of life (Fortinet, n.d.). Downstream infrastructure is relevant to refineries and

processing locations. A potential successful attack on downstream can also have a massive impact, since depending on the size of it, it can cause fuel supply shortages nationwide, financial loss and physical danger to employees or the general public (Fortinet, n.d.). Moreover, a potential attack on the corporate network can also have a significant impact, on finance (trading), data exposure (e.g. exploration and geological data) and leak of personnel information (Fortinet, n.d.).

### 3.3. Past oil & gas industry cyber security incidents

To get a better understanding of the potential impact of cyber security incidents related to the oil & gas industry, it would be useful to briefly outline a few of them, how they occurred, and what was the impact from an operational and financial aspect.

#### 3.3.1. Norsk Hydro

Norsk Hydro is a Norwegian enterprise organization with 35.000 employees that focuses mainly on Aluminum related services and products. Even though it is not an oil & gas company, it conducts business with multiple major organizations in that industry, since it specializes (amongst others) in aluminum design support in offshore and marine, as well as on extrusion technologies and friction stir welding (Hydro, n.d.). Norsk Hydro also has a strong presence into the Energy sector.

Hydro suffered one of the most recent cyber-attacks in the Energy industry. More specifically, in March 2019, Hydro was affected by a major ransomware cyber-attack. The malware was spread across 40 site locations worldwide, and it was able to encrypt critical data in servers, workstations, and laptops. The company's corporate network was brought down for preventing further spread of the ransomware virus, and services were disrupted, since the automated system of the manufacturing plant was affected, and the order processing and inventory management systems went down. The estimated cost impact was around 400-450 million NOK (41-46 million EUR) as it took more than three weeks to have all systems operating back to normal (Leppänen, et al., 2019, pp. 1,5).

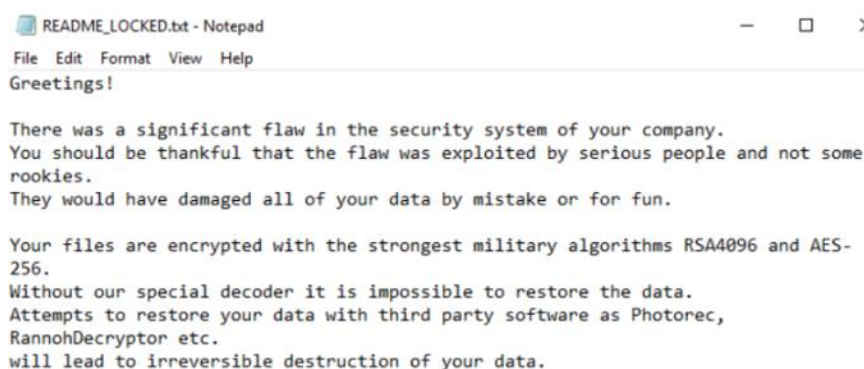


Figure 7 – Part of the post-infection note from LockerGoga virus (Leppänen, et al., 2019, p. 4)

### 3.3.2. Pemex

Pemex (Petróleos Mexicanos) is the largest petroleum company of Mexico. The state-owned petroleum organization has more than 120.000 employees, and it plays a major role in the country's economy, since it has been providing up to one third of the yearly Mexican tax revenues collected from the local government (Reuters, 2013). The company is also known for its bad environment-friendly reputation (TheGuardian, 2017), as well as for its efforts to recover from its debt in order to avoid potential credit issues (Economist, 2019).

In November 2019, Pemex was hit by a ransomware cyber-attack. The company was forced to shut down all IT systems across the corporate network, effectively bringing down all services, including payments. The ransomware responsible for the attack, was "DoppelPaymer", which was known to be affiliated with a darknet website known for ransomware attacks. The organization did not release public details regarding operational and financial impact, and it was only stated that the attack affected only 5% of the IT systems within the corporate network. According to Pemex public statements, the company refused to pay the ransom demanded by the attackers, which was 565 bitcoins (Reuters, 2019).

### 3.3.3. Saudi Aramco

Saudi Aramco is the world's biggest oil and gas organization. With an 826.8 billion USD revenue, it currently holds rank #6 in Fortune's Global 500 list (Fortune, 2020). The company has 96.000 employees worldwide, with strong global presence across Europe, America, and Asia (SaudiAramco, n.d.). On the negative side, it is responsible for 4,5% of the yearly global greenhouse emissions (TheGuardian, 2017).

In August 2012, Saudi Aramco suffered one of the worst cyber-attacks in the industry's modern era. The company has chosen to hide information related to the attack from public, however a few details have emerged during the past few years. According to information originating from a former Saudi Aramco information security advisor, it all started when one of the company's employees, opened an email with a malicious attachment. The virus started spreading across the company's clients and servers. Employees started reporting strange screen flickering on their PCs, and abnormal shutdowns. They also noticed that files started disappearing. The organizations' IT personnel decided to instantly shut down everything (a total of 35.000 computers) and disconnect all remote offices, effectively trying to block the further spread of the virus across the corporate network. Corporate emails were gone, the trading system also went down, and phone lines went dead. Employees started using typewriters and faxes as communication means. The only part which was unaffected was operations since this was an isolated and automated system. However, trucks that would try to get oil supplies were piling up, and since trading was down, they were unable to fill their tanks, therefore they started leaving. Seventeen days after the attack, Saudi Aramco started giving oil for free, since trading was still not up. It took five months to bring

their IT systems back online and the global market was affected since Aramco was producing nearly 10% of the global oil production in 2012. To deal with the threat, the company paid higher values to computer hard disk manufacturers and purchased 50.000 hard drives in replacement of their existing ones. This also caused a significant hard disk shortage and high prices worldwide (CNN, 2015).

The hackers were never caught; however, it is known that a terrorist group called “Cutting Sword of Justice” took responsibility for the attack as a response of claimed responsibilities of Saudi Arabia’s royal family for war crimes committed in Middle East countries such as Bahrain, Syria, Yemen, Lebanon and others (CNN, 2015). The financial impact is not known due to Saudi Aramco’s choice to keep information restricted.

### 3.4. Oil & gas industry “Home Office” cyber security risks

The information listed on the above subsections of the context description, can provide a clear overview of why “Home Office” generates cyber threats in the oil & gas industry. Companies conducting business in the sector choose to completely isolate the network related to plants, wells, refineries, and offshore platforms. They do so not just because of the potential financial or reputational impact, but mainly because their assets, as well as human life depends on that network, therefore it must be as isolated as possible from cyber threats. Unquestionably, the biggest threat of all, is the Internet, as that would be the most common method that potential hackers can use for reaching that network. Another major threat is the corporate network, since even though it has a lot of security layers / boundaries, it still has large exposure towards the internet mainly due to end-user experience and productivity reasons, as well as due to conducting daily tasks and communication to the outside world. It is also logical that if the internet is considered as a threat, so is the corporate network.

Up until today, most oil & gas organizations would choose to do operations such as wells, drilling or offshore platforms, or trading by using on-premise personnel. They would rarely allow employees to do such tasks remotely, because if they do so, they would have to expose these services directly or indirectly to the internet. Therefore, the exposure of such tasks to remote workers was minimal or completely absent. This changed though since the industry organizations have been forced to expose parts of those tasks to home office users. The constant growing of digitalization and cloud in the business, introduced solutions such as the digital worker (OilPrice, 2020). The former is an asset because it allows legacy tasks that would require e.g. physical paperwork, to be done digitally, while the latter enables organizations to move services to the cloud, hence making them more easily accessible from the internet, compared to on-premise legacy services. This allowed the companies to make remote working possible, even for critical tasks that used to be done from the within the organizations’ s premises. Digitalization and cloud though, also introduce risks since in many cases there is direct exposure to the internet, while access to such services relies mostly on strong authentication and role-based access of these users , rather than granting access from secured networks instead.

## 4. Research methodology

The research methodology chosen for this thesis, has a qualitative orientation. According to Hewitt-Taylor, “*the aim of qualitative research is to portray the reality of the area under investigation, and to enhance understanding of the situation and the meanings and values attributed to this by individuals; it does not involve the quantification of facts. Qualitative methods emphasize the value of individual experiences and views, as encountered in real-life situations*” (Hewitt-Taylor, 2001, p. 39).

There are many different options for conducting qualitative research. This thesis mainly utilizes literature review and the interview method.

### 4.1. Literature review

Literature review is used for establishing the theoretical basis, gathering background information related to the risk assessment standards, as well as information related to cyber security which is linked to the oil and gas industry. The material originates mainly from academic literature, online publications from cyber security vendors / experts, books, articles, and the academic material provided during the Risk Analysis and Governance MSc in the University of Stavanger. The book and article resources are selected from the University of Stavanger online library, and the choice has been done based on citations, as well as the relevance and the quality of information offered from the authors. Citations evaluation is done mainly by using the “Publish or Perish” v7 software tool, along with “Google Scholar” as the main source engine for conducting searches. Similarly, academic material offered by professors that originates from highly cited books and articles has been selected based on its relation to the research questions as well as the citation metrics in “Publish or Perish” (h-index, g-index, cites/year, total cites).

Online articles are carefully chosen, and they mostly originate from risk science and/or cybersecurity vendors and authors, from highly acknowledged web portals, linked to risk science and cyber security. Articles published by Cisco or TrendMicro for example, have been selected because these companies have been classified as top network security vendors in reviews and ratings presented in multiple Gartner rating websites (Gartner, 2021; Gartner, 2021). Gartner is an important information resource due to its wide recognition in today’s global market and its mission to provide research / advisory, and consulting services to customers (Gartner, n.d.). Facts related to COVID-19, home office, and past cyber security incidents in the oil and gas industry are taken from well-established and recognized media/news agencies such as Forbes, New York Times, The Guardian, Reuters, and others. Information related to the risk assessment methodologies are taken mainly directly from the vendors, and more specifically from the vendor papers describing the specifics of each method.

## 4.2. Interview

The interview is used as a mean for directly gathering information through cyber security experts and risk analysts, who offer their services to Equinor ASA, Norway's largest oil and gas organization. For this purpose, a questionnaire has been established (Appendix I) which has a set of questions. It was sent to the persons to be interviewed prior to the meeting, for allowing them to gather all information required, as well as for agreeing with upper management on the set of enquiries and answers they can respond to. It has four different sections. The first one is focused on the risk assessment methodologies being used by Equinor, while the second is mostly about risk assessments, emergency and/or business continuity plans related to home office and cyber security. The third section addresses facts related to "Work from Home" and cyber security, while the last one contains questions for gathering information related to common cyber threats in the oil and gas business sector.

The interview data acts as a support case study and reveals information from the organization's view, on how they dealt with the sudden large-scale home office situation. The cyber security operational experts provide an insight on how they facilitated thousands of remote users, what infrastructure changes were required, who was part of the decision-making process, and how they cooperated with risk analysis experts to provide the necessary information to the upper management, which was then used as an input before deciding on how to move forward with the home office implementation. The risk analysts provide data with regards to cyber risk assessment methodologies used, what is their experience from a "strengths / weaknesses" perspective on the methods they are utilizing, and how were the "Home Office" risk assessments conducted.

The literature and interview input will be used in this thesis as a benchmark to analyze the effectiveness of the pre-selected risk assessment methodologies while assessing and evaluating information security risks related to the "Work from Home" situation. The interview data will mostly be utilized as a case study that can provide a more realistic approach, with actual examples, for assessing the effectiveness of the methodologies. A key thing that should be noted is that the interviewed persons have chosen to provide limited information on specific questions, due to confidentiality limitations that were set by their organization prior to the interview. Moreover, the answers provided from the analysts, have been further processed by the author, to meet the needs of this thesis without modifying the core information.

### 4.3. Linking research methodologies to research questions

The first research question targets the selection of five popular information security risk assessment methodologies. It also provides a basic description of each of the preselected methods. The choice is done based on literature review, and more specifically by evaluating the frequency of appearance of these methodologies in relevant books, articles and web sites related to cyber security and risk science. However, one of the methods was also chosen due to its relevance to the Equinor case study.

The second research question is related to the identification of generic strengths and weaknesses that risk analysts, decision-makers and other stakeholders may experience while using the preselected five risk assessment methods. Research for this topic is purely based on literature review.

The third research question is based on a mix of literature review and interview-based material. It uses the input from the previous two research questions, the theory, and the context information, for assessing the effectiveness of the five risk assessment methods for the home office implementation in the oil and gas industry. More specifically, it identifies positives / negatives that risk analysts, decision-makers and other stakeholders may face while using these methods for this use-case. The interview input acts as a support case, providing real examples.

## 5. Information security risk assessments

The key thesis objective is to evaluate the suitability of risk assessment methods for identifying, evaluating, and assessing risks related to “Home Office” with a focus on the oil & gas industry. A good starting point is the identification of common risk assessment techniques being used in the global market nowadays, the selection of which is done based on literature review, such as references, citations of risk methodologies on risk science articles, web sites and books.

### 5.1. Introducing information security risk assessments

Risk analysis techniques have been growing rapidly as industries and organizations worldwide choose to proactively adapt such techniques on the way they operate their business. At the same time, information security has a unique focus from a risk perspective since several methodologies are oriented and/or tailored around cyber risk and information security. The dynamic changes in the IT world where innovations are introduced promptly, make it often difficult for other directly or indirectly related sciences to keep up. In an effort to deal with the non-static world of the IT industry, several information security risk assessment / analysis frameworks have been implemented over the past few decades, while the developers responsible for their release and maintenance, constantly evolve them in order to keep them updated and meet the most recent information security science industry standards.

There are three types of information security risk assessment frameworks, the qualitative, the quantitative, and some which are considered as a combination of both. This follows the risk analysis types description, which has been briefly analyzed in [section 2.3](#) of the thesis. From a complexity perspective, the qualitative ones are generally considered less complex, much simpler and faster to conduct, while the pure quantitative ones are the most complex, time-consuming ones, however they are known to provide solid results that are hard to challenge against. Therefore, depending on an organization’s need, or depending on the gravity and complexity of the subject to be analyzed from a risk analysis perspective, some companies might be using more than one risk assessment frameworks for their business needs.

### 5.2. Selecting common information security risk assessments

The identification and selection of the risk assessment methods to be analyzed, is mainly a result of literature review. The scope of this thesis is not to create a new risk assessment method(s), but rather to evaluate and analyze existing ones, and bring forward suggestions that could produce safer results / outcome for information security risk assessments related to “Work from Home” cyber threats. Talabis and Martin



choose to focus on ISO 27005, NIST SP800-30, FAIR, OCTAVE, ENISA, CRAMM, EBIOS and RiskIT on a similar comparison research they published in their book a few years back (Talabis & Martin, 2012, p. 13). A similar study from Agrawal, focuses on CORAS, CIRA, ISRAM and IS (Agrawal, 2017, pp. 60-61). Mnemonic AS, one of Norway's largest companies focusing on cyber threats and information security risks, lists ISO 27005, ISO 31000, IRAM<sub>2</sub>, COSO ERM, and FAIR as suggested methods (Mnemonic AS, 2020).

In general, qualitative methods seem to be more widely used because they offer a more understandable outcome and they are more time efficient. Quantitative on the other hand are mostly utilized in more complex projects, they have an objective orientation, and they offer a stronger outcome (Horvath, 2020; Goodrich, 2014). For the purposes of the thesis, three qualitative (IRAM<sub>2</sub>, OCTAVE Allegro, NIST SP800-30), one quantitative (FAIR), and one "open for customization" (ISO/IEC - ISO 27005:2018), methods have been selected. All five are included in the preidentified list of the most common ones. IRAM<sub>2</sub>, is in scope for the additional reason that Equinor ASA is using it. FAIR is chosen due to its popularity in the Fortune 1000 (FAIR Institute, n.d.). ISO/IEC - ISO 27005:2018 is widespread for its "tailoring" options and NIST SP800-30 due to its unique IT Core Infrastructure features. Finally, Octave Allegro has been selected as a widely used, open standard method for performing qualitative information security risk assessments.

### 5.3. Information security risk assessment methodologies analysis

#### 5.3.1. IRAM<sub>2</sub>

One of the most common risk assessment methodologies nowadays is IRAM<sub>2</sub> (Information Risk Assessment Methodology 2). IRAM<sub>2</sub> has been implemented by ISF (Information Security Forum) as a continuation of their original IRAM methodology. The second version though which was released in 2014, is a complete redesign, and it is a product of careful input and consultation from information risk practitioners and experts in the area. IRAM<sub>2</sub> is a "members only" information security risk assessment standard, therefore it is not open as other methodologies are. Moreover, there is a web version offering called IRAM<sub>2</sub> WebApp which is also based on the same methodology, allowing professionals to utilize an online tool for performing information risk assessments. ISF claims that IRAM<sub>2</sub> is a risk assessment model that shares many similarities with other popular methodologies, however, while others end their lifecycle on risk evaluation, IRAM<sub>2</sub> goes beyond that, offering a broader scope which also includes a pragmatic guidance on risk treatment.

The six key objectives of IRAM<sub>2</sub> are the following (ISF, 2014, p. 1):

- i. *Apply a simple, practical yet rigorous approach.* This objective outlines IRAM<sub>2</sub>'s strategy for a simplistic, practical and at the same time diligent technique, which can provide a solid, in-depth analysis, enabling organizations to perform strongly on business decision making.

- ii. *Focus on the business perspective.* IRAM<sub>2</sub> claims that the overall design of the method is focused on guiding risk practitioners towards an information risk assessment outcome with a strong business perspective emphasis.
- iii. *Obtain a greater coverage of risks.* This objective highlights the efficiency of the model on identifying all significant risk, hence drastically reducing chances of potentially missing some.
- iv. *Focus on the most significant risks.* IRAM<sub>2</sub> enables efficient resource handling from a business perspective, since it provides solid risk classification, hence allowing the business to focus primarily on the ones with the highest importance.
- v. *Speak a common language.* A key objective for IRAM<sub>2</sub> is to provide a common terminology and framework, which allows risk professionals to develop a unified view of information risk, and to offer greater integration / compatibility with the organization's enterprise risk management.
- vi. *Engage with key stakeholders.* Finally, IRAM<sub>2</sub> has a good engagement-based orientation, allowing risk professionals to involve relevant stakeholders in an organized, enterprise aware manner.

In terms of how the IRAM<sub>2</sub> risk assessment methodology is performed, it consists of six phases in total:

- I. *Phase A / Scoping.* The first phase is focused on the development of an environmental profile, as well as the definition of the assessment scope. The end goal is to provide the risk practitioner with the necessary means for obtaining a good understanding of the organization, as well as to define the scope of the assessment with the contribution of the relevant stakeholders.
- II. *Phase B / Business Impact Assessment.* During this phase, risk professionals shift their efforts on identifying information assets, and on assessing the potential impact on the business, if the identified assets are compromised. This can provide a good understanding on the environment information assets and their potential business impact ratings, for the business and the relevant stakeholders. The impact is rated in all aspects of the CIA triangle (Confidentiality, Integrity, Availability).
- III. *Phase C / Threat Profiling.* During the third phase, risk professionals and stakeholders focus on identifying risks. According to the methodology's threat definition, anything that can cause harm to an information asset by its action or inaction, is identified as a threat. This phase also includes threat profiling and prioritization, since the most critical ones need to be prioritized against others with smaller significance, while the identified threats are labeled as adversarial, accidental or environmental. Threat profiling is done based on threat attribute assessment done by the risk practitioners. Finally, the last part of this phase is to identify the information assets that could potentially be impacted by the analyzed threats.
- IV. *Phase D / Vulnerability Assessment.* The fourth phase is dedicated on assessing vulnerabilities related to pre-identified threats. By definition, a vulnerability within an environment, is a weakness in people, a process or technology. The identified vulnerabilities are mapped to each threat and are further assessed by evaluating the effectiveness of the corresponding controls.

- V. *Phase E / Risk Evaluation.* During this phase, the risk practitioners perform an evaluation of the remaining risk factors which are likelihood of success, residual likelihood, and residual business impact rating. They also derive the residual likelihood of each risk, as well as the residual risk rating, which is then used for prioritizing the risks.
- VI. *Phase F / Risk Treatment.* The last phase, is the most highlighted one of the IRAM<sub>2</sub> model, is related to the risk treatment approach, which starts with the creation of a risk treatment plan for each of the identified risks. It is mandatory for risk practitioners to be aware of the organization’s risk appetite, meaning that they should be familiar of the amount of risk(s) that the company is willing to accept. This phase also includes classification of the risks into categories depending on their origin (financial, reputational, health & safety, customer), since the organization might have set different acceptable risk limits for each of the categories.



Figure 8 – IRAM<sub>2</sub> phases

*Generic advantages / disadvantages*

In terms of generic advantages for IRAM<sub>2</sub>, it is worth noting that since it is a commercial product with a vendor supporting it, enterprise organizations can obtain much better support services, as well as access to the ISF research library, training material and numerous workshops. Moreover, many companies specializing in risk, offer IRAM<sub>2</sub> as a managed service, meaning that the organization to use it hardly ever uses its own resources. Another significant strength is the risk treatment phase, which is something that cannot be found in many other alternatives.

From a disadvantages point of view, it is worth noting that IRAM<sub>2</sub> is a “members only” risk assessment methodology, therefore it is more expensive compared to standard that are open to the community, which may be an issue for smaller companies. Moreover, the cost may rise even further if training is to be included, since this is a separate cost. Finally, the methodology may seem complex and difficult to understand for stakeholders that do not originate from the risk science / risk business area, as it may prove to be too technical for them.

5.3.2. ISO/IEC - ISO 27005:2018

ISO 27005:2018 is part of the international ISO 27000 risk management series. It provides an outline on how to conduct an information security risk assessment, according to the generic guidelines and requirements set by the standard. It is important

for organizations seeking compliance, to demonstrate the use of it on information security risk assessments. The ISO 27005:2018 standard does not specify an explicit risk management methodology, however, it defines a recurrent information risk management process, which is based on six key elements (ISO/IEC, 2018, pp. 5-20):

- I. *Context Establishment.* During the initial stages of the ISO 27005:2018 methodology, the risk practitioners focus on establishing the context, which includes criteria definition on risk identification, risk ownership responsibility, as well as how the CIA model is impacted by those risks, and how should the likelihood and impact of the identified risks should be measured. During the context establishment phase, risk experts also define the levels of risk the organization is willing to accept.
- II. *Risk Assessment.* The risk assessment phase is of great significance, since the organizations focus on their assets while developing a risk assessment process that is split into the following five sub-stages:
  - a. Compiling information assets.
  - b. Identification of threats and vulnerabilities, as well as their mapping the assets they are related to.
  - c. Use of risk criteria to calculate the impact and likelihood of each threat and/or vulnerability.
  - d. Risk evaluation against the predefined risk acceptability levels that were set during the context establishment phase.
  - e. Risk prioritization.
- III. *Risk Treatment.* During this phase, the risk experts have four different options for dealing the risks in scope:
  - a. Avoid the risk by taking measures to eliminate it.
  - b. Modify the risk by taking measures / security controls for reducing the likelihood and/or the impact, hence reducing the overall risk score.
  - c. Assign / Transfer the risk with a third party.
  - d. Retain the risk if it falls within the organization's predefined acceptable risks levels.
- IV. *Risk Acceptance.* According to the ISO 27005:2018 standard, the risk acceptance criteria need to be set by each organization, as they solely depend on policies, goals, objectives, and interests of the relevant organization stakeholders. For example, risk experts can consider risk acceptance criteria based on multiple thresholds, and if the score exceeds the threshold, senior managers can be consulted. A different example for expressing risk acceptance criteria, would be to express and evaluate the ratio of business estimated profit against the estimated risk.
- V. *Risk Communication and Consultation.* The risk communication and consultation chapter emphasize on the need of establishing and utilizing communication techniques which are the basis of information exchange between the risk practitioners and the relevant stakeholders across the organization. Risk communication is important for both normal operations, as well as emergency situations.
- VI. *Risk Monitoring and Review.* The final phase is dedicated on establishing continuous risk monitoring and review techniques, since risks can be dynamic.

Their nature might often change, new ones might be introduced, other assets might come into scope, and information security incidents may occur, therefore, it is important to take into account any changing attributes, while addressing the organization’s risk landscape.

*Generic advantages / disadvantages*

The ISO 27005:2018 standard is one of the most flexible ones in the market since it allows risk practitioners to “tailor” the methodology according to their own needs. Another strength is the reusability of it, the fact that it provides a complete risk management lifecycle, and it empowers to the risk practitioners and the stakeholders as it heavily relies of the concept of the human factor and responsibility. Lastly, the ISO standards/methodologies are well established in the market for decades, meaning that there is a lot of experience in the professional field, and organizations may use a wider set of them in other areas as well.

From a weaknesses’ perspective, ISO 27005:2018 is not an open standard as it requires membership, therefore, is can prove to be costly for small or medium sized organizations. Moreover, it does not provide a specific methodology for calculating risk, threat and impact and it leaves it open for selection to the subjective opinion of risk practitioners, which in theory could produce unreliable results. This can be perceived as a weakness by some practitioners; however, others may see it as a strength since it allows them to use whatever methodology they prefer along with ISO 27005:2018. For example, the FAIR-ISO/IEC 27005 Cookbook describes how to integrate the FAIR risk methodology model to any risk management framework (FAIR Institute, n.d.).

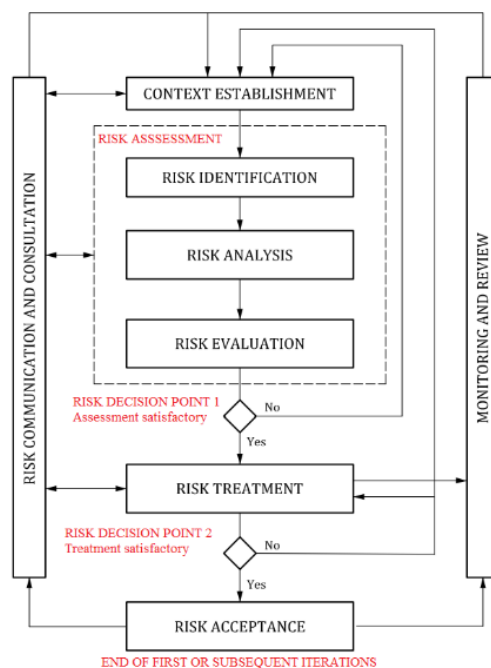


Figure 9 – ISO 27005 Information Security Risk Management Process (ISO/IEC, 2018, p. 4)

### 5.3.3. Octave Allegro

OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) was conceived in 1999 by the Software Engineering Institute of Carnegie Mellon University. The end goal was to help organizations on identifying and evaluating information security risks. In general, OCTAVE is self-directed, and it comes in alignment with Pareto's law (the 80-20 principle), which claims that 80% of the effects originates from 20 of the causes. Therefore, as a methodology, it chooses to follow the "most critical assets" risk analysis approach for prioritizing improvement areas (ComputerWeekly, 2011). It consists of three different methodologies, the OCTAVE, OCTAVE-S and the most recent OCTAVE Allegro. The latter aims to provide a streamlined process, with a clear focus on information assets, on how they are used, where they are stored, how they are transported and processed, and most importantly how due to all of the above, they end up being exposed to threats, vulnerabilities and disruptions. The developers of OCTAVE Allegro claim that this method makes all the above possible, without setting an extensive information security knowledge as a mandatory requirement. The method utilizes workshops and collaborative setups, and it can also make use of questionnaires, worksheets and guides as supporting means.

OCTAVE Allegro consists of eight steps, which are grouped into four stages (Software Engineering Institute, 2007, pp. 4-5):

- I. *Establish drivers.* During the initial stages of the OCTAVE Allegro method, the risk practitioners must develop risk measurement criteria. This is implemented in line with the organization's goals, objectives, missions, and general drivers.
- II. *Profile Assets.* The second phase is dedicated on information asset profile development, as well as information asset containers identification. According to the methodology, during this stage, risk practitioners need to profile all assets that are identified as critical. This process sets asset boundaries and it also produces asset security requirements, asset location identification and asset processing and transportation data, as a stage outcome.
- III. *Identify Threats.* Phase three is focused on identifying areas of concern, and specific threat scenarios. During this phase, risk experts shift their efforts on identifying all potential threats to the pre-identified information assets, in the context of where the assets are stored, transported, or processed.
- IV. *Identify and mitigate risks.* The final stage of the Allegro methodology is dedicated on risk identification and analysis, as well as on selecting a specific mitigation approach.

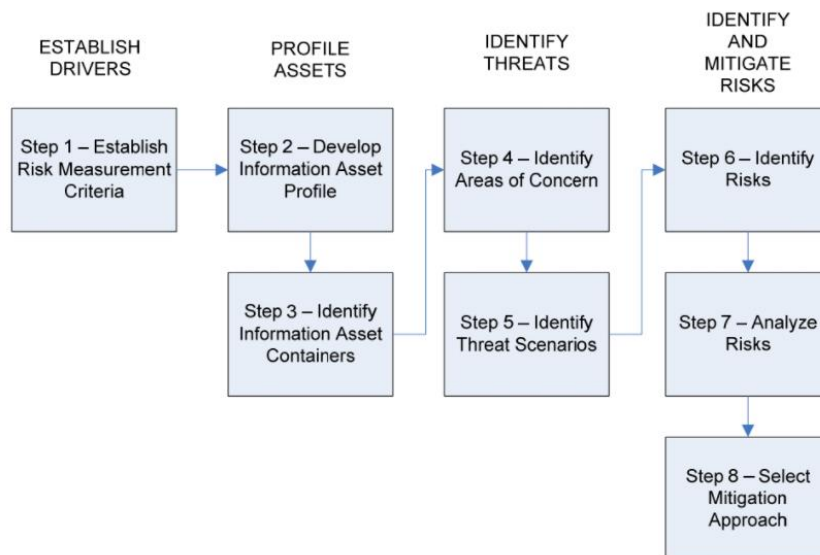


Figure 10 – OCTAVE Allegro Roadmap (Software Engineering Institute, 2007, p. 4)

#### *Generic advantages / disadvantages*

One of the strengths of the OCTAVE methodology, is that it is free, no membership is required for using it (ENISA, n.d.). That also implies that it has an open community, which can be used for information or advise exchange between companies / risk practitioners that use it. Moreover, it can be implemented in parts, allowing the organization to choose which ones should be in scope (ComputerWeekly, 2011). As a standard, it does not require focus on all assets, since it follows Pareto’s law, therefore it allows organizations to focus on what is relevant to the business context.

On the other hand, OCTAVE is a high-complexity method, since it produces high amounts of documentation which can prove difficult and time consuming for risk practitioners to process. As a qualitative method, it relies on subjectivity of the risk experts / stakeholders participating in the risk assessment process, therefore the result may prove unreliable. Moreover, even though it is a free standard that anyone may use, the tools supporting this methodology are commercial products using licensing model. The same applies for training material. Therefore, there is a cost that needs to be considered from small to medium organizations (ENISA, n.d.).

#### 5.3.4. FAIR

FAIR stands for Factor Analysis of Information Risk. It is a cyber security risk framework implemented by the FAIR institute, and its methodology fundamentally uses a quantitative approach for dealing with cyber risks. FAIR is very popular as 45% of Fortune 1000 organizations are using it, while it has more than 10.000 members worldwide (FAIR Institute, n.d.). According to the creators of FAIR, *it is the only international standard quantitative model for information security and operational risk*

(FAIR Institute, n.d.). The methodology developers are emphasizing the fact that FAIR has not been implemented to compete with other information security risk standards, but rather to join them as a complementary method that can offer the means to provide accurate information against questions such as “*How much risk does X represent*”, “*How much risk do we have*”, “*How much more/less risk will we have if...?*”, or “*What are the most cost-effective options for managing risk*” (FAIR Institute, n.d.). This comes in contrast compared to other methodologies such as the “Checklist” based ones (e.g. PCI, ISO BITS, etc.) which aim on establishing practice inventories that organizations can use for risk evaluation and benchmarking, or “CMM” methodologies (Capability Maturity Models) that mostly target process quality evaluation, setting goals and assessing the progress against them.

The FAIR methodology consists of ten steps, which are further grouped into four phases (Risk Management Insight, n.d., pp. 2-11).

- I. *Stage 1 – Identify scenario components.*
  - i. *Identify the asset at risk.* During the first step, the risk practitioner needs to identify and evaluate the specific asset(s) which is at risk.
  - ii. *Identify the threat community under consideration.* The next step of the FAIR methodology is to have the threat community identified; therefore, the risk analysts need to decide whether the threat originates from humans or malware, and if they are internal or external. As a follow-up, the risk experts also try to characterize the nature of the threat community.
- II. *Stage 2 – Evaluate Loss Event Frequency (LEF)*
  - iii. *Estimate the probable Threat Event Frequency (TEF).* Step #3 is about estimating the potential frequency within a given timeframe, that a specific threat agent can act against an asset.
  - iv. *Estimate the Threat Capability (TCap).* The Threat capability is an estimation of the probable level of force that a threat actor can have, against the asset in scope.
  - v. *Estimate Control strength (CS).* The fifth step is dedicated on calculating the effectiveness of controls that may be applied as mitigating actions. The output provides a rating of a specified control, against a baseline level of force, within a given period.
  - vi. *Derive Vulnerability (Vuln).* This step is about calculating the probability of an asset being affected from the threat agent. It is effectively a matrix calculation where Tcap (step #4) and CS (step #5) are being used on a 2-axis board.
  - vii. *Derive Loss Event Frequency (LEF).* During this step, the risk analysts take the output of steps #3 and #6 (TEF and Vuln) and produce a matrix for calculating the frequency of a potential threat harming a specific asset.
- III. *Stage 3 – Evaluate Probable Loss Magnitude (PLM)*
  - viii. *Estimate worst-case loss.* The outcome of the previous steps allows risk analysts to calculate worst case scenarios, where a specific actor acts against an asset, with the highest possible frequency, resulting in the



worst possible outcome. The magnitude of this outcome is then calculated and summed with others.

- ix. *Estimate probable loss.* The probable loss is estimated in step #9, by using a 3-step procedure. Risk practitioners identify the most likely threat community actions. As a follow-up, they calculate the probable loss magnitude for each loss form, and finally they sum up all the pre-calculated magnitudes.

IV. *Stage 4 – Derive and articulate Risk*

- x. *Derive and articulate risk.* Step #10 is the end-goal of the whole FAIR methodology. If risk analysts follow the procedure and they do effective calculations, they can provide the estimated loss event frequency (LEF) and the estimated probable loss magnitude (PLM) figures, both of which are characterized as key information for risk analysts, organizations and/or relevant risk stakeholders. The output is often demonstrated with a matrix, where LEF and PLM are using in the 2-axis board that characterizes the risk.

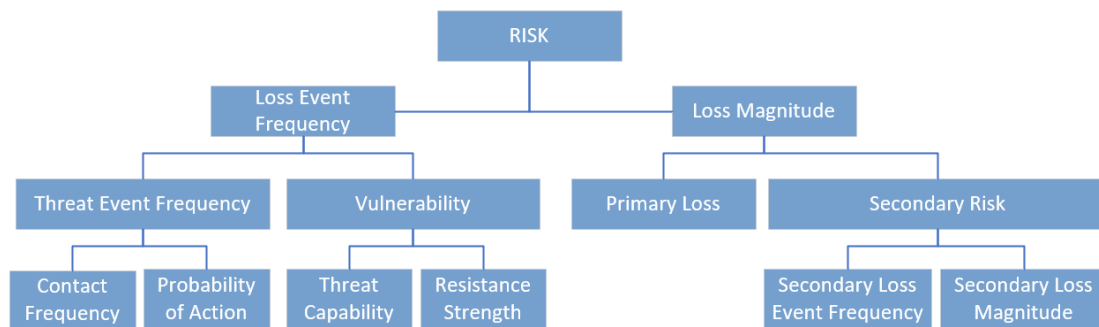


Figure 11 – The FAIR model (FAIR Institute, n.d.)

*Generic advantages / disadvantages*

FAIR is a quantitative methodology. It is therefore likely to produce very accurate results, which are hard to argue against. Moreover, the overall procedure has a good logic and it is relatively easy to understand. In addition to that, the FAIR standard is open, therefore a membership in the FAIR institute organization can provide access to the organizations which are interested on using it. Since it is widely used in enterprise-level organizations, competent and experienced resources can be found out in the market.

On the other hand, training can be costly, which could prove an impediment for small to medium organizations. Furthermore, since it is a quantitative method, it is bound to take longer in time to complete against less resource and time intensive qualitative techniques. As a methodology it has a respectful complexity level, and it may prove challenging to implement in case the risk analysts do not have sufficient metric data available. The outcome can also be hard to follow, since multiple matrix boards, directly related to each other may prove to be confusing, especially if they are presented to stakeholders unfamiliar with the concept of FAIR, or the risk science in general.

### 5.3.5. NIST SP800-30

The SP800-30 risk assessment methodology comes from the National Institute of Standards and Technology (NIST). On a broader scale, the SP800-30 special publication can be considered as an add-on / part for the NIST CSF (Cyber Security Framework), which is a well-known risk management framework in today's industry. Its purpose is to empower companies on conducting risk assessments in line with the broader NIST recommendations standards. A key characteristic of SP800-30 is the ability to assist risk practitioners on communicating with business-oriented stakeholders such as CEOs or the company's board, since it uses a common language which is easily understandable by all the involved parties (Peacock, 2020).

The methodology consists of four steps, each of which is split into several tasks (NIST, 2012, pp. L1-L2):

- I. *Step 1: Prepare for Risk Assessment*
  - *Task 1-1: Identify Purpose.* During the initial stages of the SP800-30 methodology, risk analysts must make a clear definition the risk assessment targets in terms of information to be produced, and decisions to be supported based on the outcome.
  - *Task 1-2: Identify Scope.* The next task is related to scope identification. The outcome is produced taking several factors into account, such as organizational applicability, time frame, and other considerations related to technology and architecture.
  - *Task 1-3: Identify Assumptions and Constraints.* A key task is to identify any assumptions and constraints related to the risk assessment that may affect the outcome.
  - *Task 1-4: Identify Information Sources.* During this step, risk practitioners identify information sources to be used in the risk assessment.
  - *Task 1-5: Identify Risk Model and Analytic Approach.* The final task of the first phase is to set the risk model / analytic approach that will be used as a baseline in the risk assessment.
- II. *Step 2: Conduct Risk Assessment*
  - *Task 2-1: Identify Threat Sources.* The first task of the second phase is dedicated on identification and characterization of threat sources of concern, and more specifically on the intent, capability and targeting characteristics of the threats. Based on that information, they characterized as adversarial and non-adversarial. The difference between them is that the former originates from individuals, groups, organizations, or states with a clear goal of exploitation, while the latter originates from actions that have no direct intention of causing harm / damage, such as natural disasters, or human errors.
  - *Task 2-2: Identify Threat Events.* During this task, risk analysts identify potential threat events, their relevance and threat sources that could potentially ignite those events.

- *Task 2-3: Identify Vulnerabilities and Predisposing Conditions.* The third task is devoted on vulnerabilities identification, as well as on detecting the predisposing conditions that can affect the likelihood of the threat events.
  - *Task 2-4: Determine Likelihood.* The follow up task uses the input from tasks 2-1 to 2-3 as basis, to determine the likelihood of threat events.
  - *Task 2-5: Determine Impact.* During 2-5, the risk analysts calculate the potential impact of the threat events, based on information related to their characteristics, the pre-identified vulnerabilities, and predisposing conditions, and the measures/safeguards the organization has taken for preventing such events.
  - *Task 2-6: Determine Risk.* The last task is focused on defining the risk the organization is facing, considering the potential impact from the threat events, as well as their likelihood.
- III. *Step 3: Communicate and Share Risk Assessment Results*
- *Task 3-1: Communicate Risk Assessment Results.* During the initial stages of the third phase, risk analysts use the common language framework to communicate the results towards organizational decision makers with an end goal to support risk responses.
  - *Task 3-2: Share Risk-Related Information.* The next task is dedicated on communicating / sharing the outcome produced from the risk assessment towards personnel relevant to the whole process.
- IV. *Step 4: Maintain Risk Assessment*
- *Task 4-1: Monitor Risk Factors.* During this task, risk practitioners shift their effort on monitoring pre-identified risk factors that may affect or change the risk landscape.
  - *Task 4-2: Update Risk Assessment.* As a follow up to 4-1, risk analysts conduct frequent risk assessment updates based on the monitoring output.

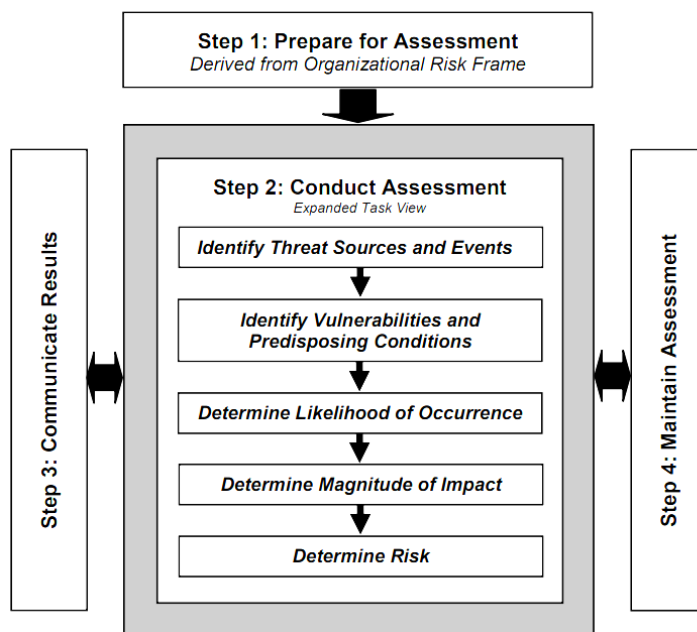


Figure 12 – NIST SP800-30 Risk Assessment Process (NIST, 2012, p. 23)

*Generic advantages / disadvantages*

One of the strongest points of SP800-30, is the effective systematic methodology it utilizes, as well as the common language framework, for cybersecurity risk treatment purposes. This enhances communication between risk analysts and business-oriented personnel involved in the risk decision-making process, as the information passed on to them is easily understandable and it can produce safer and solid decisions. Moreover, it offers good scalability and it can be used from any company / organization, regardless of its size. It is an open standard, with rich documentation. Another advantage is that NIST has been built with a focus on core IT infrastructure, therefore it can be effective on information security risk management.

From a disadvantage perspective, there is no clear definition of metrics to be used. Moreover, SP800-30 can prove complex depending on the size of the organization, as well as the predefined scope, and it is known as a difficult cyber security risk assessment framework in terms of usability. Another potential weakness is the high focus on core IT infrastructure which may prove an impediment since modern organizations choose to move away from legacy IT infrastructure, shifting towards cloud services. Moreover, since the orientation of this methodology is technical, it does not deal with some non-technical factors that should be considered (i.e. humans as organizational assets).

Risk Assessment	Type	Competence Requirements	Time Needed	Generic Advantages	Generic Disadvantages
<b>IRAM<sub>2</sub></b>	Qualitative	High	Moderate	Support	Members only
				Supporting material	Advanced skills
				Managed Service option	Complex
				Risk treatment phase	
<b>ISO 27005:2018</b>	Can be both	Standard/High	Moderate/High	Flexibility	Members Only
				Popularity, i.e. easy to find experts	Unspecified risk calculation methodology
				Reusability	
<b>Octave Allegro</b>	Qualitative	Standard/High	Moderate	Free	Complexity
				Open Community	Subjectivity dependent
				Implemented in parts	
<b>FAIR</b>	Quantitative	High	Moderate/High	Solid results	Can be time consuming
				Open standard	Result hard to follow
<b>NIST SP800-30</b>	Qualitative	Standard	Moderate	Systematic	Complexity
				Common Language	No metrics defined
				Open	IT oriented

Table 3 – Selected risk assessments generic overview (FAIR Institute, n.d.; ENISA, n.d.; NIST, 2012; ISO/IEC, 2018; ISF, 2014)

## 6. Equinor ASA case study

Equinor ASA (previously known as Statoil ASA and StatoilHydro) is Norway's largest oil & gas company, with more than 21.000 employees worldwide. It has a presence in more than 30 countries globally and a total revenue of 45.8 billion USD (Equinor ASA, 2021). Equinor is considered as a large global oil & gas player, since it has reached Fortune's Global 500 top 40 ranks twice in its recent history (Fortune, 2021). It plays a major role in the development of the Norwegian economy, as it has by far the biggest number of licenses, operatorships, operatorships fields and operatorships discoveries within the country (Norsk Petroleum, n.d.), while the petroleum and gas industry has been Norway's economy pylon in the last few decades, since it has contributed more than 15.700 billion NOK to Norway's GDP since the early 1970s (Norsk Petroleum, n.d.). Equinor has been shifting its focus in the Energy industry during the past few years, with major investments and technological discoveries. The energy related shift and innovations of the organization are much highlighted, indicating the company's efforts to switch to cleaner and more environment-friendly energy production going forward, with an end goal to contribute on the global effort of CO<sub>2</sub> emissions reduction (Equinor ASA, n.d.).

Equinor was kind enough to provide two key resources for an interview. The first one was a cyber security operations / IT infrastructure expert, while the second one was an IT infrastructure / information security risk analysis expert. Both resources and their teams played a major role during the home office implementation, which was introduced as a global measure beginning of March 2020, for protecting the health of the company's workforce, as well as for ensuring business continuity during the global pandemic outbreak.

### 6.1. Pre-“Home Office” implementation interview feedback

Equinor started looking into a potential global home office scenario, around two weeks before it was introduced. It was end of February 2020, when the company started considering this state seriously, since the outbreak started having a strong presence in Europe. Weeks before that, the organization chose to shut down their offices in Beijing, sending all local employees to work remotely from home. According to the Equinor interview resources, no workshops, risk assessments or threat simulations had been done in the past for a scenario where almost 100% of the company's global workforce would work from home. A significant effort was made though from end of February, where IT infrastructure experts were called in and received the highly prioritized task of investigating whether the organization could facilitate this project, both from a capacity / availability, as well as from a cyber security threat perspective. The plan, implementation and execution proved to be efficient for day#1 of the home office situation, however due to the limited timespan available, a few minor misses occurred, most of which were resolved during the first week of the work from home state. The

organization also implemented a business continuity plan, part of which was having almost all users working remotely.

With regards to the team that was assembled to deal with this project, the IT Infrastructure sector leader was challenged to come up with a plan for deploying a global scale home office. His response was to establish an IT “War Room”, where IT leaders, global Equinor offices representatives, operational experts, operations vendors/partners, as well as critical business areas representatives were invited. The expertise area covered remote user solutions, cyber security engineers, information security analysts, as well as network and cloud infrastructure leading advisors and experts. Critical areas of the business such as trading, exploration, drilling and offshore were also represented in the whole process.

The group managed to reach the goal of expanding the remote users’ capacity, which was mainly achieved by growing existing remote users’ solutions, as well as introducing new ones. A key success factor was that all employees had corporate managed devices, and that the company was already deeply into migrating services to the cloud, which are much easier and faster to expand. The risk management team would assess new and existing solutions, generated threats, and take actions / provide input accordingly towards decision makers. It was also noted that there were exceptions for some applications / services / tasks, where employees would only perform those with a physical presence in an office location. This was due to lack of technical solutions that could facilitate remote work for these tasks, or (in most cases) tasks that would impose a great risk if they were allowed to be executed remotely.

## 6.2. Post-“Home Office” implementation interview feedback

A set of interview questions provided an insight on the post-implementation period for Equinor. According to the interviewed personnel, most of the tasks were completed as planned and within the predefined timelines. Managers and leaders provided business support to the experts, allowing them to focus entirely on “Work from Home” related tasks. Even though there were no major challenges or barriers, two factors were identified as potential threats:

- Equinor’s dependency on vendors. If the vendors would not be able to deliver certain products in time, Equinor could have missed the deadlines that were set.
- Equinor’s dependency on operational experts. Even though there is redundancy on most operational experts, further expansion of the team could be an asset as it would remove any resource dependencies.

IT infrastructure operational experts have been following up on remote solutions that have been built, considering potential risks that are relevant to those. Mitigating actions are being taken for reducing the chances of occurrence for the identified threats, as well as their impact. Equinor experts also noted that they exchanged information with other peers / colleagues in the industry for sharing experiences, as well as for getting insights on how they dealt with the situation. Most reported that they also implemented similar solutions within less than a week, or even during a single weekend.

### 6.3. Oil & gas industry cyber security interview feedback

A set of questions was related to the cyber security for the oil and gas industry. According to the experts, the sector is threatened by common cyber security threats, which are relevant to other industries as well. What is more unique for this business area, is the type of threat actors, and more specifically the motive of a hacker. Moreover, organizations heavily rely on assets, such as onshore / offshore platforms. Therefore, the dedicated network of those assets, as well as the trading systems of an oil & gas company are critical, and most likely the top target of a potential threat actor. The technical networks related to wells are very critical as well, due to the additional fact that human life depends on them. Moreover, a potential incident may have harmful impact on the environment. Another part of the business which has IT dependencies and has a negative aftermath in case it gets compromised, is drilling, and more specifically, the software that obtains, processes and monitors drilling related data.

With regards to specific services that might generate a higher cyber security threat, the experts responded that certain services run through on-premise software platforms with high security standards / multiple security layers, due to high impact in case of a service compromise. Naturally, such tasks pose a bigger threat when the user works remotely since some security layers may not be applicable anymore. Most of those services are related to assets (e.g. offshore platforms), trading, or drilling / exploration. Moreover, there is hardware / software in Equinor which is used mainly in the oil & gas industry and is mostly related to assets (e.g. offshore), or trading of oil & gas. Cyber security intelligence gathering is done by multiple relevant teams across the organization. Equinor also gets input from relevant Norwegian government, as well as 3rd party vendors.

### 6.4. Risk assessment methodologies interview feedback

Equinor mainly uses Information Security Forum's IRAM2 for conducting cyber security risk assessments. In certain cases, the American Petroleum Institute's "Security Risk Methodology for Petroleum and Petrochemical Industries" (API 780) may also be used. These external standards have in turn been aligned with Equinor's internal management system for risk management. Both standards have been customized to fit company needs with appropriate scales for consequence assessment, threat assessment and vulnerability assessment. The combination of threat and vulnerability is used to derive a probability score for scenarios.

Equinor occasionally evaluates where the selected methodologies are efficient enough. They had two major revisions since 2014. Equinor does not have any set intervals for when to evaluate the risk assessment methodology, and this depends also on the development of applicable standards outside the company.

Regarding Equinor's experience while using these methodologies, it was highlighted that they provide a standardized way of assessing cyber risk, so that different security professionals use the same approach while comparing results, and also that these methodologies are aligned with enterprise risk management in the company overall, meaning that it's possible to compare cyber risk with any other type of risk. Equinor values that they are built from international and recognized industry standards. As an improvement point, the risk analysis expert stressed out the fact that in certain scenarios it can be very challenging to capture and describe uncertainty.



## 7. Risk assessments effectiveness on home office from an oil & gas industry perspective

The significance of assessing risks related to home office from an oil & gas industry perspective is unquestionably immense. Human life, environmental pollution and financial damage are highlighted amongst several assets that can be potentially threatened from cyber-attacks. Moreover, societies and countries can be affected from a humanitarian and financial point of view, since a successful attack could affect supplies across multiple nations.

### 7.1. Basics of evaluating risk assessment quality

According to Aven, the scientific quality of a risk assessment requires at least two perspectives for proper quality judgement: the analyst / scientist perspective, and the decision-maker's perspective, which can be expanded to include other relevant stakeholders. From a risk analyst perspective, it is important to meet some basic scientific requirements such as (Aven, 2020, p. 37):

- Work solidness, meaning it follows rules, limitations, constrains and assumptions which have been pre-identified, its logical, and in general the preselected approaches and methods have a solid justification
- Analysis relevance and usefulness, meaning it is related to the analysis target, and it contributes on solving the underlying problem.
- Assessment validity and reliability, where the former refers to the successful analysis measurements, while the latter refers to the consistency of the measuring methods. Aven highlights the importance of having both reliable and valid results. (Aven, 2020, p. 88).
- Knowledge level identification since it is important to identify knowledge or lack of knowledge in relevant areas or involved parties.
- Experience / Competence of the risk analysis team.

With regards to the decision-makers' perspective, it is important that they feel confident for the result produced from the assessment in question. Aven highlights factors that can contribute towards a stronger confidence for them and other stakeholders (Aven, 2020, pp. 37-38):

- The analysts / scientist judgement regarding the strength of knowledge that supports the results, and the potential risk of deviations from the assumptions made.
- The decision-maker's own assessment of issues related to the previous point.
- The importance of the decision-maker's understanding of the risk assessment output.
- The decision maker's judgement for evaluating the competence of the involved analysts and scientists.

Furthermore, Aven also emphasizes that decision-makers and managers do not have the necessary risk science expertise to be able to evaluate the quality of the outcome of a risk assessment, against the predefined reliability and validity criteria requirements. Risk analysts should inform them though on general topic insights, as well as a set of common validity problems which are applicable such as (Aven, 2020, p. 133):

- Important risk factors relevant to the background knowledge may be hidden.
- Risk and uncertainty assessments may be incomplete.
- Hazardous situations may be missed.

Highlighting the above to decision-makers and managers is important since they will always be responsible of the consequences of a choice, therefore it is important to understand the outcome of risk assessments and any potential constrains (Aven, 2020, p. 134).

## 7.2. Risk assessments review

The main investigation topic of this thesis is to evaluate whether the pre-selected risk assessment methods can be efficient for assessing cyber security risks related to the home office from an oil & gas industry perspective. The efficiency of those methods will be examined from a risk analysts and decision-makers point of view, therefore it will have a risk science orientation / approach.

### 7.2.1. The time factor consideration

Before conducting a specific evaluation for each of the five risk assessment methodologies, it is important to highlight a key factor, which is the time given to the oil and gas industry companies to react to the global pandemic and introduce remote work solutions for their employees. Several sources indicate that the remote work was rationally introduced within days, effectively forcing the companies to swiftly deploy these solutions in a large scale (pwc, n.d.; Norton, 2020). This comes in alignment with the Equinor case study, where the implementation of remote work solutions was done in less than ten days. The persons interviewed, mentioned that there were other peers in their industry, who introduced similar solutions in even fewer days, in some cases during a single weekend.

It can therefore be assumed that all five risk assessment methods would prove unusable, since there is simply not enough time to conduct even medium complexity risk assessments within a few days. The logical sequence of introducing a new solution for remote users would be to design it and involve risk analysts for identifying cyber security risks generated from the new solution, which would have to involve several stakeholders, technical experts, decision-makers, and other. The outcome would quite possibly take weeks, a risk treatment phase would follow, which would then lead to new evaluations. If the solution was finally accepted from higher management, it would require days (or weeks) to have it implemented. All of this seems extremely challenging

if it is to be done within a short time span. The only scenario that could prove to be realistic in a such short period, would be companies that have done similar risk assessments / workshops / simulations in the past, and they had a business continuity plan, and solutions pre-designed.

If the home office use-case is to be studied retrospectively from oil and gas organizations, there are learnings that can be harvested for two main scenarios from a time perspective. The first one would reflect the rationality this solution was introduced upon. In other words, how could a company approach a similar matter in such a short time span? The second one, assumes that there is more time to act before introducing such solutions, possibly weeks or months. The effectiveness review of the five risk assessment methodologies in this thesis, the findings, and the suggestions, offer input for both scenarios, since some observations are valid on a general basis, while others are for the specific example where the reaction time was quite limited.

### 7.2.2. Risk assessment methodologies evaluation

#### *ISF - IRAM<sub>2</sub>*

IRAM<sub>2</sub> can be very effective for evaluating cyber risks related to the oil & gas industry due to several reasons, however certain limitations need to be highlighted as well. From a duration perspective, it can provide quality results within weeks since it is not very time consuming. This is important since many oil & gas remote worker solutions are already exposed, without relying the decision to enable them, on proper risk assessment results. The business continuation rationality forced companies towards this action, however, as a post-action, it is important to investigate each remote solution separately, identify missed relevant cyber threats and take the necessary mitigating actions. If this process takes months, a potential weakness / vulnerability might be exploited, and an unwanted incident may occur. Equinor's case study also supports this approach, since it was highlighted that several issues were identified the first few weeks, most of which were fixed with follow-up mitigating actions.

Furthermore, IRAM<sub>2</sub> empowers decision-makers and business-oriented stakeholders, since it guides risk analysts towards an outcome that has a high focus on the business, which makes decision-makers more confident. Moreover, it has a common language that can be understood across the different business areas; therefore, the output of the risk assessment is clear to the involved parties. It also helps from a risk communication perspective due to the common language and framework, which are more easily understood from risk analysts that conduct similar research on non-IT related areas. Equinor's risk analysis experts mention this element as a strength that allows them to approach other risk teams within Equinor for comparing and verifying results and measurements. According to the interview, the IT War Room participants were from different areas of the business, with different backgrounds, yet they were aligned, understanding risk assessment outputs, and they contributed to solid decision-making and business continuity planning development. The involvement and active

participation of the relevant stakeholders also ensured that IT experts from different areas and responsibilities, could express their concerns on risks that might have not been identified otherwise.

Another important asset for risk analysts which is beyond the methodology suitability, is the COVID-19 / cyber risk related material which is updated from ISF and other community members with new data (ISF-Live, 2020).

From a limitations' perspective, IRAM<sub>2</sub> may prove complex to follow for new inexperienced risk analysts, or for other parties that may be involved in the conducting part of the risk assessment, since it is a methodology that requires practitioners to have a decent level of competence. This can be an issue, considering the overgrowing need of deploying new remote workers solutions, which also implies a growing demand for more highly experienced risk analysts, since existing resources may not be sufficient for carrying out pending tasks. This also imposes a higher risk for cyber security incidents, due to unknown threats that may not be identified unless a full risk assessment is conducted.

Equinor's risk analysis experts also expressed concerns regarding uncertainty, since it is often challenging to capture and describe it.

ISF IRAM <sub>2</sub>	
Strengths	Weaknesses
Time efficient	Complexity
Business focus	May prove difficult to hire competent risk analysts due to growing demand
Solid decision-making	Lack of competent resources may lead to risk assessments piling up
Common language	Pending risk assessments postpone identifying and dealing with unknown cyber threats that are present already
Effective risk communication	Uncertainty
COVID-19 related support material	

Table 4 – ISF IRAM<sub>2</sub> strengths and weaknesses on dealing with home office cyber risks (oil & gas industry perspective)

#### *ISO/IEC – ISO 27005:2018*

Just as IRAM<sub>2</sub>, ISO 27005:2018 can also prove to be effective for identifying and evaluating cyber risks related to the home office situation for oil and gas organizations. The effectiveness though depends on multiple factors, since ISO 27005:2018 does not define a risk management methodology, meaning that the risk analysts can choose to integrate qualitative / quantitative methods in it. This could prove to be an asset and an impediment at the same time, depending on the circumstances. If for example an organization is using ISO 27005 and the risk analysts were to use a qualitative risk methodology approach, they would get relatively fast results which would allow them

to investigate within weeks if the remote workers solutions that have been exposed are not vulnerable to cyber threats. However, if the organization would use a quantitative method that would be more time-consuming, they would be vulnerable for a longer period. In general, ISO 27005's flexibility would also mean that the risk analysts could change the procedure depending on the company's needs, which can be a positive factor.

Another strength of ISO 27005:2018 is ISO's popularity in the market. Equinor and several other organizations reported that they had to initiate several projects for exposing solutions to the internet for remote workers. Internet is the most preferred mean for malicious users that make attempts on compromising an organization's IT infrastructure. If the company's capacity supports dealing with X risk assessments per month, and due to COVID-19 / home office the requirement becomes Y per month, where Y is significantly higher than X, the organization needs to hire employees or consultants to deal with the situation. ISO's popularity would lead to better chances of hiring competent personnel for dealing with the company's requirements.

Another ISO 27005 strength is the fact that it heavily relies on the concept of human factor and responsibility, both of which are significant in the oil and gas industry, due to the potential consequences of severe incidents, especially with regards to human life and environmental damage.

In general, ISO 27005:2018 is challenging while evaluating its effectiveness, because of its flexibility and the ability of risk analysts to tailor the standard to their preferences. The suitability heavily depends on several options, the most important being the choice of the methodology to be integrated for estimating risk.

ISO/IEC ISO 27005:2018	
Strengths	Weaknesses
Can be time efficient	Can be time consuming
Easy to get competent / experienced resources	Uncertainty
Flexible for tailoring	
Relies on human factor and responsibility	

Table 5 – ISO/IEC ISO 27005:2018 strengths and weaknesses on dealing home office cyber risks (oil & gas industry perspective)

*Octave Allegro*

Octave Allegro has both strengths and weaknesses as a methodology, if it is to be utilized for assessing cyber threats related to home office in the oil and gas industry. Perhaps the most important advantage is the choice it provides to risk practitioners on focusing on specific assets only which are relevant to the business context. This could potentially save time for oil & gas organizations trying to identify and evaluate cyber risks for solutions that have already been rationally exposed to the internet. It is also

open / community based, therefore there is information from other peers that might provide insights in relation to the swift home office deployment.

On the other hand, there are certain weaknesses that risk practitioners need to be aware of. Octave Allegro follows Pareto’s law, which implies that around 80% of the assets in scope would be identified as related / important for the remote employees’ situation. In practice though, the rest 20% which might not be properly assessed, might impose cyber risks that could directly or indirectly damage the organization if exploited. As an example, an asset in Equinor’s case study (e.g. an offshore platform) might be left out of scope because everyone assumes that it is not exposed in any way. However, if this asset is connected with others, not exposed up to that date, and the risk owner(s) decide to make them available through the internet, the asset that was left out of scope, is now indirectly affected and may be compromised during a cyber security incident.

Another disadvantage is in relation to complexity, since Octave Allegro is known to produce significant amount of documentation, which can lead to unwanted delays while trying to evaluate the documentation data. As with the previous standards that have been reviewed in this section, time might be a significant factor if the organization is to identify cyber threats for solutions that are already exposed. Lastly, it should be emphasized that Octave Allegro is known to be heavily dependent on subjectivity, meaning that the risk analysis participants (analysts, decision-makers, operational experts and other relevant stakeholders) might have a subjective opinion on certain assets / risks, which might not be correct, therefore the results would most likely be affected.

Octave Allegro	
Strengths	Weaknesses
Can be time efficient	Can be time consuming
Focus on important / related assets only	Complexity
COVID-19 community-based data	Might miss important assets
	Subjectivity dependent
	Uncertainty

Table 6 – Octave Allegro strengths and weaknesses on dealing home office cyber risks (oil & gas industry perspective)

### *FAIR*

FAIR is the only risk assessment methodology from the ones under review, which has a quantitative orientation. It is therefore the most likely one to produce very accurate results, which would be difficult to argue against during the decision-making process. This can be a significant advantage, especially while identifying and evaluating risks related to oil and gas assets that can have major consequences in human life and the environment if they are compromised due them being exposed to the internet. Moreover, since FAIR is not a complete risk assessment framework, it can be integrated and used parallelly with others. Organizations could therefore use qualitative methods

for getting faster results on the solutions they expose to the internet and use FAIR as a follow up (or in parallel) for more accurate estimations regarding assets that may be harder to make decisions for. Another advantage is the popularity of FAIR since it is used from 45% of the Fortune 1000. This means that there are many relevant case studies or peers the risk practitioners can investigate, and it may not be a major challenge of the oil and gas organization using FAIR wants to expand the risk analysts team with experienced and competent personnel.

On the other hand, if an oil and gas company is to use FAIR as the only methodology, there are some concerns that need to be highlighted. To start off, it can be time consuming since it is quantitative, therefore the organization might be at risk until the results are available and actions / decisions are taken. Another issue is that the outcome of FAIR is known to be hard to follow, therefore not all involved parties would be able to absorb the result in an efficient way. This may lead to problematic decision-making as well. FAIR is heavily dependent on proper and accurate input / metrics, therefore, if the risk analysts do not have that, the result might be flawed.

FAIR	
Strengths	Weaknesses
Solid results help on decision-making	Time consuming
COVID-19 community-based data	Organization may be at risk due to time needed
Can be used in parallel, or as part of other methodologies	Results hard to understand
Easier to increase risk analysts' personnel due to popularity	Uncertainty

Table 7 – FAIR strengths and weaknesses on dealing home office cyber risks (oil & gas industry perspective)

#### *NIST SP800-30*

NIST SP800-30 demonstrates its effective systematic methodology as one of its strongest points. This can help risk analysts working in the oil and gas industry on producing reliable and valid results. It also enables decision-makers on making proper decisions with regards to cyber risks relevant to remote working solutions / projects that have been exposed already. Furthermore, just as IRAM<sub>2</sub>, NIST SP800-30 uses a common language framework. Data is easily understandable across risk analysts, decision-makers, and other stakeholders with different background (business/finance oriented, IT, drilling, offshore operational experts). Another advantage that needs to be highlighted is that NIST SP800-30 is “Core IT infrastructure” oriented. Oil and gas companies are still using legacy core IT infrastructure designs due to the nature of the applications which are relevant to the industry, as well as their decision to keep some of those applications isolated from the rest of the organization’s core network, and the internet for security reasons. Therefore, NIST SP800-30 seems to be tailored for

companies that rely on legacy core IT infrastructure designs and prefer to keep several services within their own data centers rather than moving them to the Cloud.

On the other hand, risk analysts working for oil and gas organizations need consider the fact that NIST SP800-30 is known to be a complex model, and just as ISO 27005:2018, it does not have specific metrics defined. Therefore, from a procedural perspective, depending on the use-case, it may be hard to follow especially for decision-makers or stakeholders that do not have a risk science background / experience. Another important observation is that the NIST SP800-30 standard has a high IT orientation, and it may not be possible to consider or value non-IT factors. This can be an issue for oil and gas organizations since for example human life and environmental impact, are assets that can prove to take into account. Another factor that should be reflected upon, is the core IT infrastructure orientation potential unsuitability if some of the services in scope are cloud based. NIST SP800-30 has not been recently revised and may therefore have flaws while assessing risks for cloud-based services. This could lead into potential misses, which endanger the company’s assets. Equinor’s case study reveals that oil and gas organizations have chosen to move several services to the cloud. Therefore, risk analysts that consider using SP800-30 for evaluating cyber risks for the oil and gas industry, need to evaluate if the modern “Hybrid” model (Core IT Infrastructure + Cloud) is suitable for this specific risk assessment model.

NIST SP800-30	
Strengths	Weaknesses
Effective systematic methodology	Complexity
Common language framework	Organization may be at risk due to time needed
Understandable output	Results hard to understand
Core IT infrastructure oriented	May be unsuitable for Hybrid or Cloud IT Infrastructure models
	Uncertainty

Table 8 – NIST SP800-30 strengths and weaknesses on dealing home office cyber risks (oil & gas industry perspective)



## 8. Discussion

### 8.1. Findings

An important factor that needs to be considered retrospectively for determining the effectiveness of the pre-selected risk assessments for the home office reality in the oil and gas industry, is time. Companies had a limited timespan for assessing cyber risks properly, therefore, none of the risk assessment methodologies would be effective, unless there was relevant past data that could speed up the process. Based on Equinor's case study, decision-makers, top managers, risk owners, operational experts, and other stakeholders, acted within a few days with an end-goal of building a business continuity plan based on working from home, while the risks were assessed on the fly. Due to this, as a continuation, organizations would have to conduct full risk assessments for each of the developed solutions, while time has again a significant importance, since solutions were already exposed to the internet without having the full risk picture before exposing them. Equinor's story verifies this finding, as there were some minor misses, most of which were followed up and resolved from the risk analysts and cyber security operational experts.

Due to the rationality of introducing and expanding remote work solutions, follow-up risk assessments would be needed. IRAM<sub>2</sub>, Octave Allegro and NIST SP800-30 could produce a faster outcome, which would help organizations on securing their home office solutions from potential risks that were not identified prior to introducing them. ISO 27005:2018 could also prove time effective, depending on how the risk analysts choose to tailor the solution and its metrics. FAIR would be more challenging since it is quantitative, therefore, it would most likely take more time for conducting an assessment based on that methodology. This implies that the company would be at risk for a greater period, until the output is available, and actions are taken. It could be used though for relevant projects / solutions, where a qualitative risk analysis result would not be sufficient for decision-makers and they would require stronger, objective output before taking decisions.

Moreover, there are important findings worth highlighting from a risk analysts / decision-makers / stakeholders perspective, which are applicable on a broader scale, meaning that they are valid, in scenarios where companies would have a much larger time span to react upon and do proper planning both for developing remote work solutions, as well as for conducting relevant risk assessments. IRAM<sub>2</sub> can offer a complete risk lifecycle to risk analysts, including a risk treatment phase. It also has a strong business orientation, something which can be highly appreciated by decision makers and/or risk owners in oil and gas organizations with a business background, since it usually helps them produce quality decision-making results. An extra asset is the common language, which enhances risk communication. A potential impediment can be complexity, as it is not an easy methodology to conduct and follow, and it requires highly experienced and competent risk analysts. If there is a sudden high-volume of risk assessments, it can be challenging to expand the risk analysts' team on time.

ISO 27005:2018 is the biggest question mark of this research, since its high customization / tailoring capabilities can prove to be both an asset, as well as an impediment. However, in principle, it can prove very useful for oil and gas organizations, since it relies on human factor and responsibility, which are attributes highly appreciated in that industry. It can also integrate both quantitative and qualitative methodologies, providing one common framework to risk analysts which can be used in almost any use-case / project.

Octave Allegro's characteristics can help companies get results relatively fast, which is a benefit in situations where results are needed in haste, however an important weakness is that it can be complex as a method, and more importantly, it can miss or misjudge the value of specific assets, hence exposing the company to potential risks with an unknown impact. This is very important for oil and gas organizations, where human life and the environment are at stake from a potential cybersecurity incident. Another important factor is that Octave Allegro relies heavily on the subjectivity of the participants, which could produce unsafe results depending on their competence, as well as their view and understanding of certain attributes.

FAIR's strongest advantage is that the results it produces are hard to question, therefore, it makes a decision-maker's life a lot easier, which can prove important in the home office / oil and gas industry use-case. On the other hand, besides the time factor that has already been mentioned, the results can sometimes be difficult or complex to understand properly.

NIST SP800-30 is perhaps the most IT-oriented methodology, and that comes with advantages. The output can be easily understood, from IT-oriented stakeholders / experts, and it uses a core-IT infrastructure orientation, which appears to be close to the legacy IT infrastructure designs that oil & gas companies have. It also uses a common language framework that can be understood across the relevant stakeholders, and it has an effective and systematic orientation. However, it may introduce challenges as well, since it can be complex, and the results can be difficult to understand for decision-makers and stakeholders without a technical background. Moreover, the risk analysts and operational experts need to evaluate its suitability against more modern IT models, such as the "Hybrid" ones which combine legacy designs with Cloud IAAS (Infrastructure as a Service).

Furthermore, some findings need to be emphasized in terms of reliability and validity as well. On a general basis, qualitative methodologies are quite dependent on the subjectivity of the participants, therefore, results produced by them can be questionable. As an example, an organization might use two teams consisting of risks analysis / decision-makers / stakeholders for assessing the risk of exposing a solution to the internet for operating an offshore platform remotely. According to a cyber security expert who is part of the first team, the likelihood of having a remote client compromised by an attacker is 0,1%, however, another operational expert on the second team considers 0,01% as a more proper probability metric. This is subjective in both cases, and if risk analysts consider the same impact score for both cases, the first time will produce a risk score which is ten times higher compared to the one produced from the second team. Therefore, there is no reliability on the results, and some (if not all)

may be invalid as well. IRAM<sub>2</sub>, Octave Allegro and NIST SP800-30 (ISO 27005:2018 as well depending on its customization) could potentially be vulnerable to this issue due to their qualitative nature. On the other hand, a quantitative approach such as FAIR, can also introduce challenges, since it may be difficult to characterize and deal with risk and uncertainties (Aven, 2020, p. 85). However, it would most likely produce reliable and valid results, because its much less dependent on subjectivity. A pure quantitative methodology though can be all about numbers, which is also problematic according to Aven, since risk cannot be characterized and expressed solely by numbers and the results might be difficult to follow (Aven, 2020, p. 84).

Another finding is related to the importance of relevant data a company would possess prior to the home office implementation. Such input could drastically reduce the input needed from experts for developing such projects and dealing with the generated risk. Equinor was fortunate to have data from the home office implementation for Beijing users, which was a few days in advance. This action provided important insight on potential issues and risks that would be faced while extending the remote employees scenario on a global scale. Other organizations built similar solutions in a smaller time span, without having a previous experience. Another scenario would be companies that have done a past case study / simulation, where all employees would work remotely due to a threat of a different nature. Such simulation could provide important insight on relevant cyber risks.

## 8.2. Suggestions

If a time constrain is to be considered for a similar use-case in the future, a logical approach would be to do a rational evaluation of the existing data and examine the possibility of re-using information from past risk assessments that are related. If an IT solution is already exposed, it most probably implies that the decision was made in accordance to governing rules, risk assessment findings and relevant follow-up actions. Past risk assessment input that can be used for producing rapid results by using the five methodologies examined, can be an option, however, not a likely one if the available period is a few days only.

In such rational situations, risk assessment methodologies that could prove more suitable would be the rapid risk assessments (RRA). A rapid risk assessment can take hours or in certain cases minutes to complete. RRA is not a full risk / vulnerability assessment methodology, but rather a high-level one. Its main objective is to estimate the value and impact of a specific service to the reputation, finances and the productivity of the project or business in scope. It is suitable for such circumstances because of its speed, and its simplistic nature, therefore it can be easily understood by the involved parties (Mozilla, n.d.). The main weakness of RRAs, is that they can often produce invalid measurements and invalid results / outcomes, due to their rational nature.

A logical approach in hasty use-cases would be to use RRAs for a quick analysis of the cyber risks related to home office, expose the solutions needed for business continuity, and then use a full risk assessment methodology that normally produces results within

a few weeks, for re-assessing each of the solutions that were made available on the internet. This approach seems to be the one followed from Equinor also, since the solutions were swiftly re-examined after their initial introduction.

From a risk assessment perspective, it would be hard to recommend one methodology only for rational use-cases, since it would seem more proper to use at least two, if not three under such scenarios. RRA seems more fit for the initial pre-service-publishing phase. IRAM<sub>2</sub>, NIST SP800-30 and ISO 27005:2018 (under specific circumstances) seem more suitable for re-assessing these services after their initial exposure. FAIR can be used if decision-makers need more solid results which are harder to question before taking actions related to a specific “Work from Home” service. Therefore, a “One solution that fits all” option, may not be the best one for the cyber risks’ analysis related to the home office implementation from oil & gas organizations. Aven also has a similar suggestion, indicating that there are considerable limitations by using exclusively pure qualitative or quantitative methodologies, and he further suggests that a combined quantitative/qualitative approach can be a better option as it merges the strengths of both worlds and it minimizes their weaknesses (Aven, 2020, pp. 84-85).

On the other hand, if a company has much more time to react upon, all five methodologies can prove useful, but some seem more suitable against others. There are only a few limitations that have been identified for IRAM<sub>2</sub>, and FAIR, that should be considered. NIST SP800-30 has the extra limitation of not being able to value certain non-technical assets, such as human life, which may prove more challenging for oil & gas organizations. ISO 27005:2018 can be effective, but this highly depends on how the risks analysts customize it. Octave Allegro on the other hand, has one limitation that needs to be seriously considered, and that is the Pareto’s law approach. Petroleum companies seem to have a strong emphasis on evaluating all their assets properly, therefore this methodology may prove inefficient due to potential misses. Therefore, ideally risk analysts could follow a qualitative approach by using IRAM<sub>2</sub>, ISO 27005:2018 or NIST SP800-30, and utilize quantitative techniques such as FAIR if a stronger, objective results is required from the decision-makers and extended time is available.

Another obvious suggestion is to conduct simulations of similar crisis scenarios. Companies can develop business continuity plans, pre-designed IT solutions and pre-conducted cyber security risk assessments, have them on stand-by, and review them periodically. This could be done for example for a scenario of a complete company offices lockdown, which would imply that personnel required to have a physical presence in the corporate network for operating critical offshore or drilling solutions, would not be allowed to do so, therefore only home office would be applicable even for such critical tasks.

Even though the technical part is relatively out of scope for this thesis, it is worth highlighting some elements that could prove valuable while implementing large-scale home office solutions. Based on Equinor’s study, an easy approach is to extend existing remote users’ solutions as much as possible, since they are already exposed, and relevant risk assessments have been conducted in the past prior to exposing them. Cloud migrations can also be an asset, since some of the key advantages of such services is

scalability and business continuity implementation with minimal effort, (Queensland Government, n.d.). An important ingredient towards a successful and swift home office implementation can be company-owned and managed devices such as laptops, since the organization can apply strict security policies and have a good insight on security events generated from these devices.

Based on the thesis findings, a generic pattern can be suggested depending on the time availability, as well as the characteristics and complexity of an industry and/or a project in scope. For example, oil and gas companies tend to often perform exhaustive risk assessment techniques since human life, as well as the environment is at stake. The same cannot be assumed for other industries, such as retail. There are common observations though, regardless of the complexity of the business area or the project. If time is limited, only RRAs are applicable. For a relatively average time availability, qualitative methods can be used. However, as the timespan grows, companies should consider using a mix of qualitative/quantitative techniques, which can be most effective for more challenging tasks. The following figure demonstrates the generic pattern mentioned above:

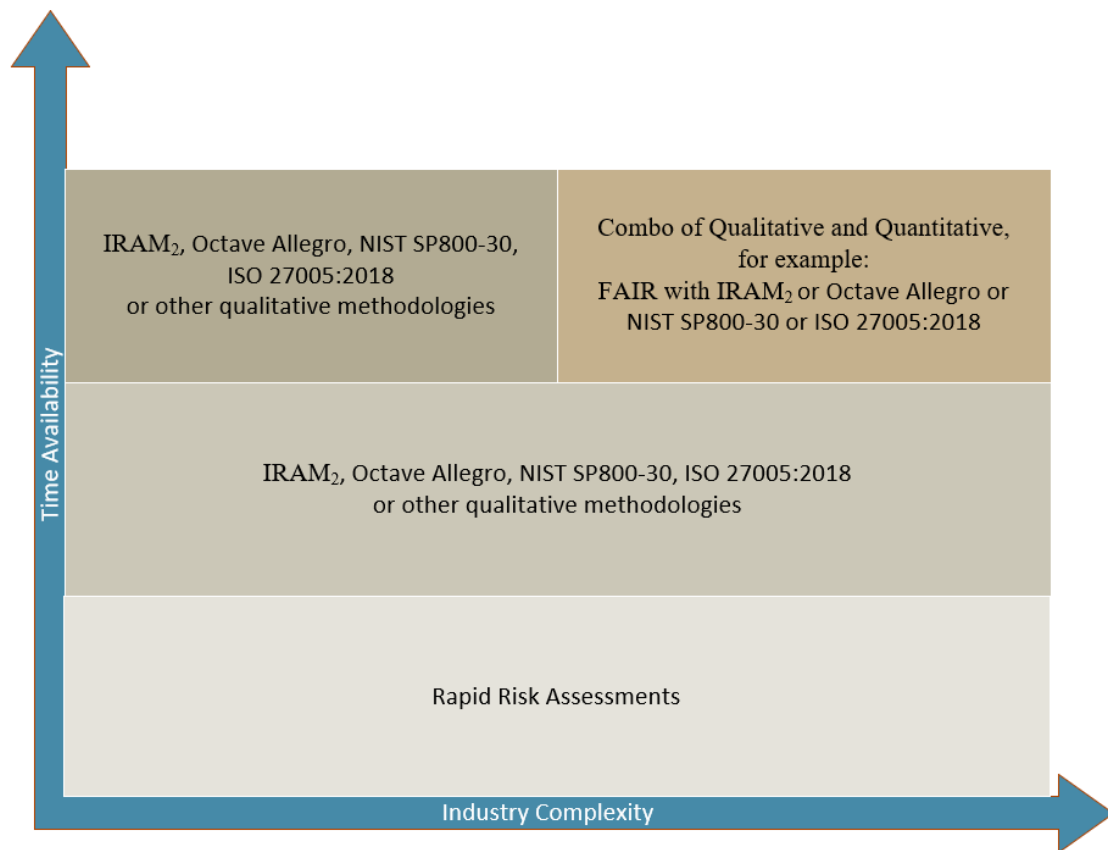


Figure 13 – Suggested risk assessment methodologies depending on time availability and industry complexity.

### 8.3. Future research

Research on this thesis can be further expanded in multiple angles. The obvious one is to include more risk assessment methodologies, providing a holistic review that could assist risk analysts on understanding specific strengths and weaknesses for each, while using them as tools for conducting cyber security risks assessments related to home office for the oil and gas industry.

The study field can also be expanded to focus on home office in general, however this can prove quite challenging since there are different characteristics for each industry. Retail for example is mostly related to business-to-client or business-to-business shopping/sales, therefore the potential impact from cyber security risks is very different. That implies that there might be different strengths or challenges that risks analysts, decision-makers and stakeholders need to consider while using the five risk assessment methodologies included in this thesis.

Another consideration is having the vendors / creators of those methods, reviewing, and evolving them, releasing new versions in the market, with improvements and/or potential weaknesses. In such a scenario, parts of this research may not be applicable anymore due to the new characteristics of one or more of those methodologies.

Finally, more relevant case studies could be included in a future research providing a complete picture with a bigger real-examples sample. This could potentially provide other findings / solutions / suggestions, that can prove valuable as well.

## 9. Conclusions

There are many learnings that can be absorbed, some of which have a higher significance compared to others. From a risk science perspective, each method has generic strengths and weaknesses. Depending on the characteristics of the company and the industry it belongs to, some of the generic positives or negatives, may have a bigger or smaller impact. There are also advantages and impediments to consider when time is a major factor.

For the home office situation in the oil and gas industry, it seems that the best approach for risk analysts would be to possess experience on at least two or more risk assessment types and use them accordingly depending on the use-case. A similar future incident that would give oil and gas companies a wider period to react upon, could potentially utilize one methodology only. A rational scenario would most likely utilize two or three different. From the investigated ones, IRAM<sub>2</sub> and FAIR may prove a strong combination of one qualitative and one quantitative methodology, which should cover most needs. The other ones can also prove usable if the risk analyst is aware of the limitations they have.

A key factor for successfully introducing new solutions and for properly following risk assessment methodologies, is proactiveness. This is applicable not just for the oil and gas industry, but for any business sector in general. Identifying cyber threat scenarios, simulating network breaches, examining the possibility of a scenario that would not allow employees to reach the corporate offices (for example environmentalists blocking entrance to all office locations for an oil and gas company), building business continuity and risk treatment plans, are things that can provide valuable data, which may prove very useful during potential extreme situations.

## Bibliography

Agrawal, V., 2017. A Comparative Study on Information Security Risk Analysis Methods. *Journal of Computers*, 12(1), pp. 57-67.

Aven, T., 2015. *Risk Analysis*. 2nd ed. West Sussex: John Wiley & Sons, Ltd.

Aven, T., 2020. *The Science of Risk Analysis - Foundation and Practice*. 1st ed. New York, London: Routledge.

Aven, T. & Vinnem, J.-E., 2007. *Risk Management: With Applications from the Offshore Petroleum Industry*. 1st ed. New Jersey: Springer.

BBC, 2020. *Coronavirus: France's first known case 'was in December'*. [Online] Available at: <https://www.bbc.com/news/world-europe-52526554> [Accessed 20 February 2021].

BusinessNewsDaily, 2019. *Steve Jobs Biography*. [Online] Available at: <https://www.businessnewsdaily.com/4195-business-profile-steve-jobs.html> [Accessed 27 May 2021].

Calder, A. & Watkins, S., 2015. *IT GOVERNANCE – AN INTERNATIONAL GUIDE TO DATA SECURITY AND ISO27001/ISO27002*. Sixth edition ed. London, Philadelphia, New Delhi: KoganPage.

Canadian Centre For Cyber Security, 2020. *Canadian Centre for Cyber Security - An Introduction to the Cyber Threat Environment*. [Online] Available at: <https://cyber.gc.ca/sites/default/files/publications/Intro-to-cyber-threat-environment-e.pdf> [Accessed 21 March 2021].

Cisco, 2020. *Cisco Cybersecurity Report Series 2020 - CISO Benchmark Study*. [Online] Available at: [https://www.cisco.com/c/dam/global/en\\_uk/solutions/security/UK-CISO-Benchmark-Report-2020.pdf](https://www.cisco.com/c/dam/global/en_uk/solutions/security/UK-CISO-Benchmark-Report-2020.pdf) [Accessed 17 April 2021].

CNN, 2015. *The inside story of the biggest hack in history*. [Online] Available at: <https://money.cnn.com/2015/08/05/technology/aramco-hack/index.html> [Accessed 24 April 2021].

CNSS, 2015. *CNSSI 4009 Committee on National Security Systems (CNSS) Glossary*. [Online] Available at: <https://www.serdp-estcp.org/Tools-and-Training/Installation-Energy-and-Water/Cybersecurity/Resources-Tools-and-Publications/Resources-and-Tools-Files/CNSSI-4009-Committee-on-National-Security-Systems-CNSS-Glossary> [Accessed 21 March 2021].

ComputerWeekly, 2011. *OCTAVE risk assessment method examined up close*. [Online]



Available at: <https://www.computerweekly.com/tip/OCTAVE-risk-assessment-method-examined-up-close>  
[Accessed 30 April 2021].

Devopedia, n.d. *Information Security Principles*. [Online]  
Available at: <https://devopedia.org/information-security-principles>  
[Accessed 13 May 2021].

DigitalGuardian, 2020. *The Ultimate Guide to BYOD Security: Overcoming Challenges, Creating Effective Policies, and Mitigating Risks to Maximize Benefits*. [Online]  
Available at: <https://digitalguardian.com/blog/ultimate-guide-byod-security-overcoming-challenges-creating-effective-policies-and-mitigating>  
[Accessed 18 April 2021].

Economist, 2019. *Latin America's state-run oil giants are struggling*. [Online]  
Available at: <https://www.economist.com/business/2019/07/13/latin-americas-state-run-oil-giants-are-struggling>  
[Accessed 20 April 2021].

ENISA, n.d. *Octave*. [Online]  
Available at: [https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m\\_octave.html](https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_octave.html)  
[Accessed 30 April 2021].

Equinor ASA, 2021. *Where we are*. [Online]  
Available at: <https://www.equinor.com/en/where-we-are.html>  
[Accessed 8 May 2021].

Equinor ASA, n.d. *The Energy Transition. The defining opportunity of our time*. [Online]  
Available at: <https://www.equinor.com/>  
[Accessed 9 May 2021].

EU, n.d. *What is GDPR, the EU's new data protection law?*. [Online]  
Available at: <https://gdpr.eu/what-is-gdpr/>  
[Accessed 13 March 2021].

FAIR Institute, n.d. [Online]  
Available at: <https://www.fairinstitute.org/frequently-asked-questions>  
[Accessed 2 May 2021].

FAIR Institute, n.d. *FAIR FAQ*. [Online]  
Available at: <https://www.fairinstitute.org/frequently-asked-questions>  
[Accessed 2 May 2021].

FAIR Institute, n.d. *HOME OF FAIR / THE STANDARD QUANTITATIVE MODEL FOR INFORMATION SECURITY AND OPERATIONAL RISK*. [Online]  
Available at: <https://www.fairinstitute.org/>  
[Accessed 2 May 2021].

FAIR Institute, n.d. *The FAIR Model*. [Online]  
Available at: [https://cdn2.hubspot.net/hubfs/1616664/The%20FAIR%20Model\\_FINAL\\_Web%20Only.pdf](https://cdn2.hubspot.net/hubfs/1616664/The%20FAIR%20Model_FINAL_Web%20Only.pdf)  
[Accessed 2 May 2021].

FAIR Institute, n.d. *WHAT IS FAIR?*. [Online]  
Available at: <https://www.fairinstitute.org/what-is-fair>  
[Accessed 2 May 2021].

Fortinet, n.d. [Online]  
Available at: <https://www.fortinet.com/fr/solutions/industries/oil-gas#use-case-3>  
[Accessed 19 April 2021].

Fortinet, n.d. [Online]  
Available at: <https://www.fortinet.com/fr/solutions/industries/oil-gas#use-case-4>  
[Accessed 19 April 2021].

Fortinet, n.d. *Oil and Gas Cybersecurity - Overview*. [Online]  
Available at: <https://www.fortinet.com/fr/solutions/industries/oil-gas#overview>  
[Accessed 18 April 2021].

Fortinet, n.d. *Securing Midstream Infrastructure*. [Online]  
Available at: <https://www.fortinet.com/fr/solutions/industries/oil-gas#use-case-2>  
[Accessed 19 April 2021].

Fortune Business Insights, 2021. *Cyber Security Market Size, Share & COVID-19 Impact Analysis, By Component (Solution and Services), By Deployment Type (Cloud and On-Premise), By Enterprise Size (Small & Medium Enterprise and Large Enterprise), By Industry (BFSI, IT and Telecommunication)*. [Online]  
Available at: <https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165>  
[Accessed 17 April 2021].

Fortune, 2020. *Global 500 - Saudi Aramco*. [Online]  
Available at: <https://fortune.com/company/saudi-aramco/global500/>  
[Accessed 24 April 2021].

Fortune, 2021. *Equinor*. [Online]  
Available at: <https://fortune.com/company/statoil/global500/>  
[Accessed 9 May 2021].

Gartner, 2020. *Gartner Survey Reveals 82% of Company Leaders Plan to Allow Employees to Work Remotely Some of the Time*. [Online]  
Available at: <https://www.gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82-percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time>  
[Accessed 17 April 2021].

Gartner, 2021. *Endpoint Protection Platforms (EPP) Reviews and Ratings*. [Online]  
Available at: <https://www.gartner.com/reviews/market/endpoint-protection-platforms>  
[Accessed 31 May 2021].

Gartner, 2021. *Network Firewalls Reviews and Ratings*. [Online]  
Available at: <https://www.gartner.com/reviews/market/network-firewalls>  
[Accessed 31 May 2021].

Gartner, n.d. *About us*. [Online]  
Available at: <https://www.gartner.com/en/about>  
[Accessed 31 May 2021].

Gartner, n.d. *Connected Home*. [Online]  
Available at: <https://www.gartner.com/en/information-technology/glossary/connected-home>  
[Accessed 18 April 2021].

Gartner, n.d. *Gartner Glossary - Bring Your Own Device (BYOD)*. [Online]  
Available at: <https://www.gartner.com/en/information-technology/glossary/bring-your-own-device-byod>  
[Accessed 17 April 2021].

Gartner, n.d. *Internet Of Things (iot)*. [Online]  
Available at: <https://www.gartner.com/en/information-technology/glossary/internet-of-things>  
[Accessed 18 April 2021].

GlobalData, 2019. *Oil and gas sector continues to rule 2019 Fortune Global 500 list in revenue generation, finds GlobalData*. [Online]  
Available at: <https://www.globaldata.com/oil-and-gas-sector-continues-to-rule-2019-fortune-global-500-list-in-revenue-generation-finds-globaldata/>  
[Accessed 18 April 2021].

Goodrich, B., 2014. *Qualitative Risk Analysis vs Quantitative Risk Analysis*. [Online]  
Available at: <https://www.pmlearningsolutions.com/blog/qualitative-risk-analysis-vs-quantitative-risk-analysis-pmp-concept-1>  
[Accessed 4 June 2021].

HelpNetSecurity, 2020. *4.83 million DDoS attacks took place in the first half of 2020, a 15% increase*. [Online]  
Available at: <https://www.helpnetsecurity.com/2020/09/30/4-83-million-ddos-attacks-first-half-of-2020/>  
[Accessed 21 March 2021].

Hewitt-Taylor, J., 2001. Use of constant comparative analysis in qualitative research. *Nursing standard: official newspaper of the Royal College of Nursing*, 15(42), pp. 39-42.

Horvath, I., 2020. *Difference Between Qualitative and Quantitative Risk Analysis*. [Online]  
Available at: <https://www.invensislearning.com/blog/qualitative-vs-quantitative-risk->

analysis/

[Accessed 4 June 2021].

Hydro, n.d. *Aluminium is ideal for offshore*. [Online]

Available at: <https://www.hydro.com/en/aluminium/industries/solar-and-energy/oil-and-gas/>

[Accessed 20 April 2021].

Infosecurity Magazine, 2020. *#COVID19 Drives Phishing Emails Up 667% in Under a Month*. [Online]

Available at: <https://www.infosecurity-magazine.com/news/covid19-drive-phishing-emails-667/>

[Accessed 17 April 2021].

Investopedia, 2020. *What Percentage of the Global Economy Is the Oil and Gas Drilling Sector?*. [Online]

Available at: <https://www.investopedia.com/ask/answers/030915/what-percentage-global-economy-comprised-oil-gas-drilling-sector.asp>

[Accessed 18 April 2021].

Investopedia, 2021. *How the Oil and Gas Industry Works*. [Online]

Available at: <https://www.investopedia.com/investing/oil-gas-industry-overview/>

[Accessed 18 April 2021].

Irwin, L., 2021. *The cyber security risks of working from home*. [Online]

Available at: <https://www.itgovernance.co.uk/blog/the-cyber-security-risks-of-working-from-home>

[Accessed 13 May 2021].

ISF, 2014. *IRAM2 - The next generation of assessing information risk*. s.l.: Informa on Security Forum Limited.

ISF-Live, 2020. *ISF CISO COVID-19 Recovery Resource Suite*. [Online]

Available at: <https://www.isflive.org/s/covid-19-resource-centre>

[Accessed 15 May 2021].

ISO 31000:2018, 2018. *ISO 31000:2018(en) / Risk management — Guidelines*.

[Online]

Available at: <https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en>

[Accessed 30 March 2021].

ISO/IEC, 2018. *Information Technology - Security Techniques - Information Security Management*. Geneva: ISO.

Jackson, J. K., Weiss, M. A., Schwarzenberg, A. B. & Nelson, R., 2020. *Global Economic Effects of COVID-19*, s.l.: Congressional Research Service.

Kaspersky Labs, n.d. *What is VPN? How It Works, Types of VPN*. [Online]

Available at: <https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn>

[Accessed 18 April 2021].

- Kaspersky Labs, n.d. *COVID-19: How to stay safe from hackers and avoid Coronavirus scams*. [Online]  
Available at: <https://www.kaspersky.com/resource-center/threats/coronavirus-how-to-stay-safe-hackers-scammers>  
[Accessed 17 April 2021].
- Kastner, E., 2021. *TOP 5 REMOTE WORK CYBER SECURITY RISKS [2021]*. [Online]  
Available at: <https://www.soscanhelp.com/blog/remote-work-cyber-security-risks>  
[Accessed 13 May 2021].
- Kosutic, D., 2016. *Where does information security fit into a company?*. [Online]  
Available at: <https://advisera.com/27001academy/blog/2016/10/24/where-does-information-security-fit-into-a-company/>  
[Accessed 20 March 2021].
- Kosutic, D., 2016. *Where does information security fit into a company?*. [Online]  
Available at: <https://advisera.com/27001academy/blog/2016/10/24/where-does-information-security-fit-into-a-company/>  
[Accessed 13 May 2021].
- Leppänen, S., Suvi, A. & Granqvist, R., 2019. *Cyber Security Incident Report — Norsk Hydro*. [Online]  
Available at:  
[https://mycourses.aalto.fi/pluginfile.php/923542/mod\\_folder/content/0/Group%20CS%20Norsk%20Hydro%202019.pdf](https://mycourses.aalto.fi/pluginfile.php/923542/mod_folder/content/0/Group%20CS%20Norsk%20Hydro%202019.pdf)  
[Accessed 20 April 2021].
- Mnemonic AS, 2020. *Agile Security Strategy*. [Online]  
Available at: <https://www.mnemonic.no/no/security-report-2019/agile-security-strategy/>  
[Accessed 25 April 2021].
- Mozilla, n.d. *Rapid Risk Assessment*. [Online]  
Available at: [https://infosec.mozilla.org/guidelines/risk/rapid\\_risk\\_assessment.html](https://infosec.mozilla.org/guidelines/risk/rapid_risk_assessment.html)  
[Accessed 15 May 2021].
- NIST, 2012. *NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments*. [Online]  
Available at: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>  
[Accessed 3 May 2021].
- Norsk Petroleum, n.d. *Companies*. [Online]  
Available at: <https://www.norskpetroleum.no/en/facts/companies-production-licence/>  
[Accessed 9 May 2021].
- Norsk Petroleum, n.d. *The government's revenues*. [Online]  
Available at: <https://www.norskpetroleum.no/en/economy/governments-revenues/>  
[Accessed 9 May 2021].

Norton, J., 2020. *Businesses Need to Rethink Cyber Risks for Work-from-Home Employees*. [Online]

Available at:

<https://www.insurancejournal.com/news/national/2020/09/17/582888.htm>

[Accessed 15 May 2021].

O' Reilly, n.d. *APPENDIX C: A 5X5 RISK MATRIX FOR SEVERITY AND LIKELIHOOD*. [Online]

Available at: [https://www.oreilly.com/library/view/establishing-an-occupational/9781787781429/xhtml/Appendix\\_C.html](https://www.oreilly.com/library/view/establishing-an-occupational/9781787781429/xhtml/Appendix_C.html)

[Accessed 4 April 2021].

OilPrice, 2020. *The Oil And Gas Industry Is Going Remote*. [Online]

Available at: <https://oilprice.com/Energy/Crude-Oil/The-Oil-And-Gas-Industry-Is-Going-Remote.html>

[Accessed 24 April 2021].

Outpost24, 2020. *Press Release: Over half of organisations have no visibility into the number of devices on their wireless network, Outpost24 Survey Finds*. [Online]

Available at: <https://outpost24.com/Press-Release-Over-half-of-organisations-have-no-visibility-into-the-number-of-devices-on-their-wireless-network-Outpost24-Survey-Finds>

[Accessed 18 April 2021].

Peacock, J., 2020. *What is NIST SP 800 30*. [Online]

Available at: <https://securityboulevard.com/2020/06/what-is-nist-sp-800-30/>

[Accessed 3 May 2021].

pwc, n.d. *COVID-19: Making remote work productive and secure*. [Online]

Available at: <https://www.pwc.com/us/en/library/covid-19/making-remote-work-productive-secure.html>

[Accessed 15 May 2021].

Queensland Government, n.d. *Benefits of cloud computing*. [Online]

Available at: <https://www.business.qld.gov.au/running-business/it/cloud-computing/benefits>

[Accessed 24 May 2021].

Reuters, 2013. *Mexico to keep pumping Pemex for tax money despite promised reforms*. [Online]

Available at: <https://www.reuters.com/article/mexico-reforms-pemex-idUSL1N0IB0OI20131030>

[Accessed 20 April 2021].

Reuters, 2019. *Hackers demand \$5 million from Mexico's Pemex in cyberattack*. [Online]

Available at: [Hackers demand \\$5 million from Mexico's Pemex in cyberattack](#)

[Accessed 20 April 2021].

Risk Management Insight, n.d. *FAIR Basic Risk Assessment Guide*. [Online]

Available at:

[https://web.archive.org/web/20101122083435/http://www.riskmanagementinsight.com/media/docs/FAIR\\_brag.pdf](https://web.archive.org/web/20101122083435/http://www.riskmanagementinsight.com/media/docs/FAIR_brag.pdf)  
[Accessed 2 May 2021].

SaudiAramco, n.d. *Who we are - Global presence*. [Online]  
Available at: <https://www.aramco.com/en/who-we-are/overview/global-presence>  
[Accessed 24 April 2021].

Shell, n.d. *What We Do*. [Online]  
Available at: <https://www.shell.com/about-us/what-we-do.html>  
[Accessed 18 April 2021].

Singer, P. W. & Friedman, A., 2014. *Cybersecurity and Cyberwar - What everyone needs to know*. New York: Oxford University Press.

Software Engineering Institute, 2007. *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*. Boston: Carnegie Mellon University.

SRA, 2018. *Society for Risk Analysis Glossary*. [Online]  
Available at: <https://www.sra.org/wp-content/uploads/2020/04/SRA-Glossary-FINAL.pdf>  
[Accessed 30 March 2021].

Talabis, M. R. M. & Martin, L. J., 2012. *Information Security Risk Assessment Toolkit - Practical Assessments through Data Collection and Data Analysis*. 1st ed. Boston: ELSEVIER.

Tennant, F., 2020. *The COVID catastrophe: labour and unemployment*. [Online]  
Available at: <https://www.financierworldwide.com/the-covid-catastrophe-labour-and-unemployment#.X57AX4j0ljE>

TheGuardian, 2017. *Just 100 companies responsible for 71% of global emissions, study says*. [Online]  
Available at: <https://www.theguardian.com/sustainable-business/2017/jul/10/100-fossil-fuel-companies-investors-responsible-71-global-emissions-cdp-study-climate-change>  
[Accessed 20 April 2021].

TrendMicro, 2015. *The Case of Making BYOD Safe*. [Online]  
Available at: <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/the-case-for-making-byod-safe>  
[Accessed 18 April 2021].

TrendMicro, 2019. *IoT Devices in the Workplace: Security Risks and Threats to BYOD Environments*. [Online]  
Available at: <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/iot-devices-in-the-workplace-security-risks-and-threats-to-byod-environments>  
[Accessed 18 April 2021].

TrendMicro, n.d. *Drilling Deep: A Look at Cyberattacks on the Oil and Gas Industry*. [Online]  
Available at: <https://www.trendmicro.com/vinfo/us/security/news/internet-of->

things/drilling-deep-a-look-at-cyberattacks-on-the-oil-and-gas-industry  
[Accessed 20 April 2021].

Verizon, 2020. *2020 Data Breach Investigations Report*. [Online]  
Available at: <https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf>  
[Accessed 21 March 2021].

Whitmain, M. E. & Mattord, H. J., 2011. *Principles of Information Security*. Fourth Edition ed. Boston: Cengage Learning.

WHO, 2020. *Listings of WHO's response to COVID-19*. [Online]  
Available at: <https://www.who.int/news/item/29-06-2020-covidtimeline>  
[Accessed 20 February 2021].

WHO, 2021. *WHO Coronavirus Disease (COVID-19) Dashboard*. [Online]  
Available at: <https://covid19.who.int/>  
[Accessed 20 February 2021].

WTO, 2020. *Trade set to plunge as COVID-19 pandemic upends global economy*. [Online]  
Available at: [https://www.wto.org/english/news\\_e/pres20\\_e/pr855\\_e.htm](https://www.wto.org/english/news_e/pres20_e/pr855_e.htm)



## Appendix

### Appendix I – Interview questionnaire

#### Questions on the risk assessment methodologies

1. Which risk assessment method(s) are you using for analyzing cyber security threats?
2. Is the risk assessment method(s) used as-is, or has it been customized to fit your company's needs? If so, please provide a brief description of these customizations.
3. How often does the company evaluate whether the selected risk assessment model(s) is efficient enough?
4. Please outline strengths and weaknesses that have been experienced with the risk assessment models that have been utilized by your company to the date.
5. Does the company have one common risk analysis team for evaluating cyber security risks / threats related to remote working, or are there multiple teams?
6. If there are multiple teams, are they all using the same risk assessment model or do they use different ones?

#### Questions on risk assessments, emergency plans and/or business continuity plans, related to COVID-19 "Home Office" and cyber security

1. Has a risk Assessment been done in the past, for evaluating potential cyber security risks related to home office? If so, was the case of having most employees working from home included in the pre-defined scenarios?
2. If the scenario of having most employees working remotely was investigated, was a risk treatment plan also implemented?
3. Did the company's emergency plan / business continuity plan investigate the shift to remote working and to what extent?
4. Was a risk assessment done after the COVID-19 outbreak, before introducing "Home Office" for the company's employees?

#### Questions related to the "Home Office" situation

1. Was the company's IT infrastructure prepared and equipped to handle the global "Work from Home" situation caused by the COVID-19 pandemic?
2. What is the percentage of the company's personnel that works using remote solutions?
3. Were the IT resources sufficient and prepared on day #1 of the "home office" situation?

4. Please provide a high overview of the IT crisis response team (participants, business areas etc.)
5. Were the activities relevant to the sudden and large-scale shift to remote working executed as planned, or were there any challenges? If so, how were they dealt with?
6. Does the company conduct follow-up risk assessments for potentially identifying new threats and risks that might emerge during the “Work from Home” period? If so, how often?

#### Questions related to cyber security in the oil and gas industry

1. Please outline cyber security risks / threats which are relevant and unique for the oil and gas industry.
2. Are there any tasks related to the oil and gas industry, that generate a high cyber security risk / threat, if they are to be conducted remotely from home? Please describe a number such tasks along with a brief explanation of the potential impact in case of an incident, and mitigating actions for reducing the overall risk score of these threats.
3. Does your company utilize cyber security / cyber defense technologies which are tailored for the oil and gas industry?
4. How does your company gather intelligence / information related to potential Cyber threats?
5. What is the company’s strategy for cyber security and Working from Home going forward? Does the strategy include plans for allowing remote work even for traditional tasks that would normally require an on-site presence of the employee?