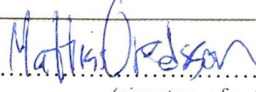




Universitetet  
i Stavanger

FACULTY OF SCIENCE AND TECHNOLOGY

## MASTER'S THESIS

Study programme/specialisation: Risk management	Spring / Autumn semester, 20.18.  Open/Confidential
Author: Mattias Oredsson	 ..... (signature of author)
Programme coordinator: Roger Flage  Supervisor(s): Stian Sviggum	
Title of master's thesis: Bridging the gap between information security risk assessments and enterprise risk management – how to ensure a balanced reporting of information security risks to the top management and the board.	
Credits: 30	
Keywords: Information security, risk assessment, IRAM <sub>2</sub>	Number of pages: ..... 63 ..... + supplemental material/other: .....  Stavanger, 15.05.18 ..... date/year

# **Bridging the gap between information security risk assessments and enterprise risk management**

How to ensure a balanced reporting of information security  
risks to the top management and the board

## Abstract

It is challenging to feed today's information security risk assessments into an overall ERM framework such that it can be presented to stakeholders and management. This report evaluates current practice for information security risk assessment as represented by IRAM<sub>2</sub>, which is a recognised methodology. Weaknesses have been revealed in IRAM<sub>2</sub> related to its incompatibility with other reporting methods, and in its calculation methods of information risks. Improvements have been proposed to the inherent limitations of the methodology, but also how to increase IRAM<sub>2</sub>'s compatibility with other risk management models.

## Acknowledgements

The process of writing this thesis has been a challenge from start to finish. It would not have been possible without the continuous support and guidance from my two supervisors; Roger Flage, professor of risk analysis at the University of Stavanger, and Stian Sviggum, director at PricewaterhouseCoopers AS. I would also like to thank my brother for always making sure that I raise the level of my work.

# Table of contents

<b>List of figures</b> .....	<b>vi</b>
<b>List of tables</b> .....	<b>vi</b>
<b>1 Introduction</b> .....	<b>1</b>
1.1 Objectives, scope and limitations .....	1
1.2 Report structure .....	1
<b>2 Risk theory</b> .....	<b>2</b>
2.1 The concept of risk .....	2
2.2 Risk characterisation .....	3
2.3 Risk matrices .....	4
2.4 Information risk in the context of enterprise risk management.....	5
<b>3 Information security risk management</b> .....	<b>8</b>
3.1 Confidentiality, integrity and availability .....	8
3.2 Threat, asset and vulnerability .....	8
3.3 Frameworks and standards for risk management and information security.....	10
3.4 IRAM <sub>2</sub> methodology .....	11
3.4.1 Phase A: Scoping .....	12
3.4.2 Phase B: Business Impact Assessment.....	13
3.4.3 Phase C: Threat Profiling .....	15
3.4.4 Phase D: Vulnerability Assessment .....	22
3.4.5 Phase E: Risk Evaluation .....	25
<b>4 Evaluation of IRAM<sub>2</sub></b> .....	<b>29</b>
4.1 Concepts .....	29
4.2 Comparison with ISO 31000.....	32
4.2.1 Principles .....	32
4.2.2 Process.....	34
4.3 Methods .....	36
4.3.1 Calculation methods .....	36
4.3.2 Risk output .....	38
4.3.3 Background knowledge and uncertainty .....	39
4.4 Other.....	40
4.5 Conclusion.....	41
<b>5 Improving IRAM<sub>2</sub> and information security risk assessments in general</b> .....	<b>42</b>
5.1 Criteria for strength of knowledge .....	43
5.2 Risk scoring system.....	45
5.3 Other improvements .....	47
<b>6 Discussion</b> .....	<b>48</b>
6.1 Overall considerations .....	48
6.2 Bridging the gap .....	49
6.3 Further work .....	50
<b>7 Conclusion</b> .....	<b>53</b>
<b>8 References</b> .....	<b>54</b>

## List of figures

Figure 1 - ERM hierarchy .....	6
Figure 2 - Three-factor approach .....	9
Figure 3 – IRAM <sub>2</sub> assesses information risk .....	11
Figure 4 - Flowchart IRAM <sub>2</sub> methodology.....	12
Figure 5 - Flowchart of IRAM <sub>2</sub> .....	37
Figure 6 - InfoSec risk output and enterprise risk output .....	39
Figure 7 – Connection between operational risk and IRAM <sub>2</sub> .....	42
Figure 8 - BN for IRAM <sub>2</sub> .....	52

## List of tables

Table 1 - Example risk matrix .....	5
Table 2 - Business Impact Reference Table (BIRT).....	13
Table 3 - Impact scenario assumptions.....	14
Table 4 - Business impact assessment template .....	15
Table 5 - Common threat list (CTL).....	16
Table 6 - Threat Profiling Reference Table (TPRT).....	18
Table 7 - Threat profiling template.....	19
Table 8 - Prioritised threat landscape.....	20
Table 9 - Threat event catalogue (TEC) (excerpt).....	21
Table 10 - Determining the basis for each information risk equation .....	22
Table 11 - The extent of control relevance .....	23
Table 12 - Control relevance table.....	24
Table 13 - Extent of implementation of control.....	24
Table 14 - Control implementation assessment.....	25
Table 15 - Recorded information risk equation .....	26
Table 16 - Likelihood of success (LoS) matrix .....	27
Table 17 - Residual likelihood matrix .....	27
Table 18 - Residual risk rating matrix .....	28

Table 19 - Residual risk profile with SoK judgement .....	44
Table 20 – IRAM <sub>2</sub> risk factor scoring table.....	45
Table 21 - Proposed risk scoring table.....	46
Table 22 - Residual risk profile with SoK judgements for likelihood and impact .....	49

# 1 Introduction

Organisations are faced with increased organisational complexity and a broad range of threat vectors that may interfere with their operations and objectives. Enterprise risk management (ERM) covers the methods and procedures that can be used to manage the risks posed by these threats. The focus on proper risk management, and the framework that contains it, is increasing throughout all types of industries. However, because of the different risk types that exist within an organisation there are several approaches for assessing risk, and it can be challenging for an organisation to successfully align these approaches when they are implemented into the preferred overall framework.

As a consequence of our society's increased application and dependency on information technology, the importance of information security is increasing. The information risks and cyber threats faced by organisations today are constantly evolving and growing at a quick pace. Nowadays, hacking services are bought and sold on places such as the Darknet. This leads to an exponential increase in threats, as the services are readily available to anyone. A hacker that once was characterised as a kid sitting in front of the computer in the basement, has now transformed into established, well-funded professionals. To keep up, organisations need to take a proactive approach against these threats (Oredsson, 2017). Therefore, it is crucial to have a robust mechanism in place that can properly communicate these risks and provide decision support to the top management. However, it is challenging to feed today's information security risk assessments into an overall ERM framework such that it can be presented to stakeholders and management. There is potential for improvement of current methodologies for this translation of risk from information security to the overall risk management framework.

## 1.1 Objectives, scope and limitations

The objective of this report is to evaluate current practice for information security risk assessment as represented by IRAM<sub>2</sub>, provide suggestions on how to improve this methodology and to find ways of advancing how these information risks are reported to the decision makers. The scope of the assignment will be delimited to IRAM<sub>2</sub>. However, as the methodology is based on known principles within information security, the evaluation and proposed improvements will, to some degree, be applicable to the information security field in general.

## 1.2 Report structure

Firstly, risk theory is presented to build the foundation on which the suggestions will lean on. Information security, typical frameworks and standards are then introduced, before the IRAM<sub>2</sub> methodology is presented. Evaluation of the methodology follows, and then the suggestions for improvements. The report ends with a discussion and some suggestions for further work.



## 2 Risk theory

Risk analysts are often faced with the challenge of describing or characterising risk that an organisation faces in an informative but simple manner for the management and the stakeholders. The analyst could be assessing different types of risks, such as if they are security or safety related. Depending on the scope, different perspectives and characterisations of risk are used. It is therefore of interest to introduce recommendations on risk conceptualisation. This will establish the foundation for this thesis.

[Section 2](#) presents general theory on risk, discusses risk as a concept and how risk can be described, and briefly presents risk management within enterprises.

### 2.1 The concept of risk

The concept of risk has no universally accepted definition (Aven, 2014, p. 17). For example, some definitions are based on expected values, while others might be based on probabilities. The term “risk” is used loosely and has different context-dependent meanings. This can be challenging for risk practitioners that need to communicate risk to stakeholders and can also lead to ineffective risk management, as many of the definitions lack legitimate scientific support (Aven, 2011b).

As stated by Aven (2011b), despite the need for customised risk methods, procedures and models, there is no justification for having different perspectives on how to think regarding risk and uncertainty. The challenge remains the same, which is to conceptualise that the future performance of a system or an activity could lead to outcomes different from those desired and planned, or not in line with stated objectives (Aven, 2011b, p. 1).

There have been many variations of the risk concept over the years. One of the most common conceptualisations of risk in use today is the (C,P) perspective, where C is the consequences and P refers to the related probabilities of the consequences. This conceptualisation is often used in ERM and the risk is usually characterised by risk matrices. The perspective on risk where probability is one of the main dimensions can be challenged by the fact that probability is an imperfect tool and can produce inadequate predictions. This perspective does not acknowledge that the probabilities are conditioned on several assumptions and beliefs. Uncertainties can be hidden in this background knowledge, and by limiting awareness to just the probabilities can conceal crucial factors that could produce surprising outcomes (Aven, 2010).

For a comprehensive historical coverage the reader is pointed to the work by Aven (2014). The perspective taken in this report is based on Aven’s recommendations. It is stated in (Aven, 2017) that a general perspective like what the author advocates captures most of the common definitions of risk and is also in accordance with the Society for Risk Analysis (SRA, 2015). The following way of representing risk separates the concept of risk and how it is described or characterised.

Consider an activity, e.g., investing in a new start-up company, opening a new online store or travelling to a new location. These activities lead to unknown consequences (C). At present time it cannot be established what the consequences will be – they are uncertain (U). The risk concept advocated by Aven (2017) consists of these two main features: consequences C in relation to the values of interest and the related uncertainties (U). The definition outlined does not differentiate between positive and negative consequences, which leads to a more objective approach to risk. This is because categorising the consequences as either positive or negative would introduce the opinion of the assessor, and that could be problematic since what is considered an undesirable outcome for one stakeholder, does not necessarily mean that this view is shared by the others.

Adopting the two-dimensional (C,U) perspective (also called the general risk approach) allows for any type of uncertainty representation, which means it can work as a unified perspective on uncertainties in a risk assessment context (Aven, 2014, p. 34). The perspective supports concepts like surprises and black swans (surprising extreme event relative to the present knowledge/beliefs (Aven, 2013, p. 6)) and is also consistent with the belief that decision-making under risk and uncertainties should be risk-informed, not risk-based. The (C,U) perspective distinguish the concept of risk and how it is measured or described, which should encourage an approach that is more humble in the search of what risk entails (Aven, 2014, p. 38).

The consequences are often divided into events A and consequences C. Risk is then written as (A,C,U) (Aven, 2015, p. 13). The risk concept is now defined. However, this concept is not used as a tool for assessing risk. To measure or describe risk, a risk characterisation, or description, must be established.

## 2.2 Risk characterisation

Having provided the risk concept, the recommended framework for describing risk can now be specified. Risk characterisation, or risk description, is defined in SRA (2015) as a qualitative and/or quantitative picture of the risk; i.e., a structured statement of risk usually containing the elements:

- risk sources
- causes
- events
- consequences
- uncertainty representations/measurements (for example probability distributions for different categories of consequences – casualties, environmental damage, economic loss etc.)
- the knowledge that the judgements are based on.

As defined in the [Section 2.1](#), risk has two dimensions, consequences and uncertainties. The risk description is realised by specifying the consequences and using a description, or measure, of the uncertainty, Q. There are various ways to measure uncertainty (Aven, 2014, p. 69), such as:

The statistical approach that uses frequentist probabilities (the frequentist probability of an event A is interpreted as the fraction of times A occurs if the experiment could be repeated infinitely many times under similar conditions (Aven, 2017)).

The Bayesian approach, where uncertainty is represented by subjective probabilities (judgemental or knowledge-based probabilities, characterised by an individual's personal degree of belief whether a specific outcome is likely to occur (Oredsson, 2017, p. 4) or using frequentist probabilities (referred to as chances in this setting) which are parameters of probability models that support the assignment process of subjective probabilities.

General risk approach, here any representation (measure) of uncertainty Q, for example probability P or imprecise probabilities.

Specifying the consequences entails identification of quantities of interest C', which characterise the consequences C. The value of the C' is of interest in the risk analysis because they give information regarding the performance of the alternatives that are considered. The quantities C' are predicted in the risk analysis, and the uncertainties are assessed. The general description of risk can now be obtained (Aven, 2015, p. 14):

Risk description = (A'C',Q,K), where

A' is some specified events and K is the background knowledge that Q and C' are based on.

This framework recognises that risk is more than just probabilities and expected values. The uncertainty dimension extends beyond the probabilities and the framework assists in providing crucial input for making judgements regarding the quality of risk assessments (Aven, 2011b, p. 9).

### 2.3 Risk matrices

Risk matrices are widely used to characterise risk in enterprise risk management frameworks and is also used to characterise information risks in the methodology used as a case study for this report. This section will therefore give a brief introduction to the risk matrix.

A risk matrix is a table with categories for impact or consequence on the x-axis, and categories for likelihood or probability on the y-axis. The intersection between each category on the x-axis and each category on the y-axis signifies a risk level (Cox, 2008) and is often colour coded to signify the magnitude of risk. Usually, the consequences are related to negative outcomes such as monetary losses or fatalities. As can be seen from Table 1, the resultant risk of the consequence-probability pair (<\$10M,<5% per year) is in the green colour category, which normally signifies a low risk. On the other hand, the resultant risk of the consequence-

probability pair (>\$100M,>50% per year) is in the red colour category, which signifies a high risk.

<b>Probability</b>	>50% per year				
	20%-50% per year				
	5%-20% per year				
	<5% per year				
		<\$10M	\$10M- \$50M	\$51M- \$100M	>\$100M
<b>Consequence (financial loss)</b>					

**Table 1 - Example risk matrix**

Risk matrices are commonly used by organisations as a decision-support tool in risk management (Flage & Røed, 2012), and is also a prevalent tool for presenting the risk picture in enterprise risk management frameworks. Some of the main advantages of the risk matrix is that it is intuitive, easy to understand and does not require any formal education to make use of it. However, the idea that the matrix can satisfactorily capture the full risk picture with two dimensions – consequence and probability – has been challenged (e.g. (Aven, 2017)) partly because it does not reflect the knowledge dimension. Despite receiving criticism over the years (e.g. (Cox, 2008), (Flage & Røed, 2012)), the risk matrix is still widely used to describe risk.

#### 2.4 Information risk in the context of enterprise risk management

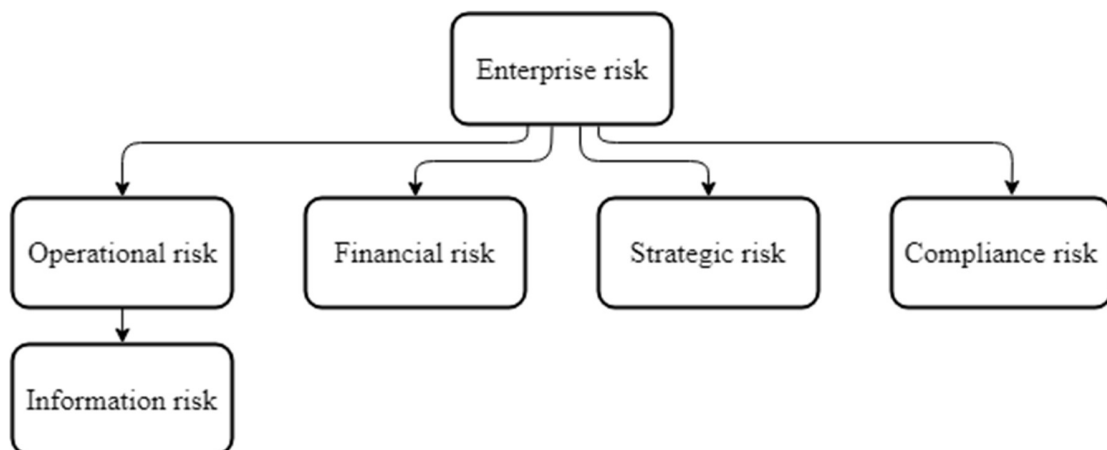
The purpose of this section is to give an overview and to establish the context for information risks.

Risk management relates to all activities, conditions and events that can affect the organisation and its ability to reach the organisation’s goals and vision (Aven, 2015, p. 4). Risk management specifically in enterprises is a relatively new field of risk (D’Arcy & Brogan, 2001) and there are, albeit similar, several definitions on what enterprise risk management entails. The ERM definition adopted here is the Casualty Actuarial Society Enterprise Risk Management Committee definition (2003):

“ERM is the discipline by which an organization in any industry assesses, controls, exploits, finances, and monitors risks from all sources for the purpose of increasing the organization’s short- and long-term value to its stakeholders.”

There are many benefits associated with the implementation of an ERM-framework. It can increase opportunities, identify risks throughout the company, and increase the company’s profit while reducing negative consequences. Risk management in enterprises is commonly divided into risk categories such as organisational risk, financial risk, strategic risk and compliance risk (Information Security Forum, 2017, p. 5). Although the categories can vary to some degree, the primary point is that enterprise risk management considers all types of risk an organisation faces (D’Arcy & Brogan, 2001, p. 4).

A traditional conceptualisation of risk in risk management models is the (C,P) perspective, where C is the consequences and P refers to the related probabilities of the consequences. At the corporate level, the standard approach for describing risks in most risk management models is using risk matrices. Individual risks are assessed in terms of risk level, which is a function of the consequences of an event and the likelihood (probability/frequency). When presenting the total risk picture for the organisation, the idea is to compare risks from all departments, e.g. combining quantitative assessments in finance with quantitative risk assessments regarding production, to support decision making at the corporate level.



**Figure 1 - ERM hierarchy**

Operational risk is risk where the consequences for the enterprise are a result of safety- or security-related issues such as accidental events and intentional acts (Aven, 2015, p. 5). Basel Committee on Banking Supervision (2011) defines operational risk as:

“The risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.”

An overview of the ERM hierarchy with a focus on the sub-domain of information risk is shown in Figure 1. For the purpose of this report it is of interest to investigate information risk, which can be thought of as a sub-domain of operational risk (Information Security Forum, 2017, p. 5).

## 3 Information security risk management

The main goal of information security is to ensure business continuity and minimise business damage by preventing and minimising the impact of security incidents (von Solms, 1998, p. 224). To achieve this goal, there must be a functioning risk management process in place. This entails having a systematic approach to information security risk management (ISRM) that identifies organisational needs in relation to information security requirements and to create an effective information security management system (International Organization for Standardization, 2011).

Information security is defined by The International Organization for Standardization (2017) as: “preservation of confidentiality, integrity and availability of information”. Preserving the confidentiality, integrity and availability of information can be critical for e.g. maintaining competitive advantage and cash flow. This means that there is a need to protect data and system assets that are essential for the business from those who could potentially misuse it. To understand how information risk is assessed, the concept of confidentiality, integrity and availability, and the three-factor approach will be presented.

### 3.1 Confidentiality, integrity and availability

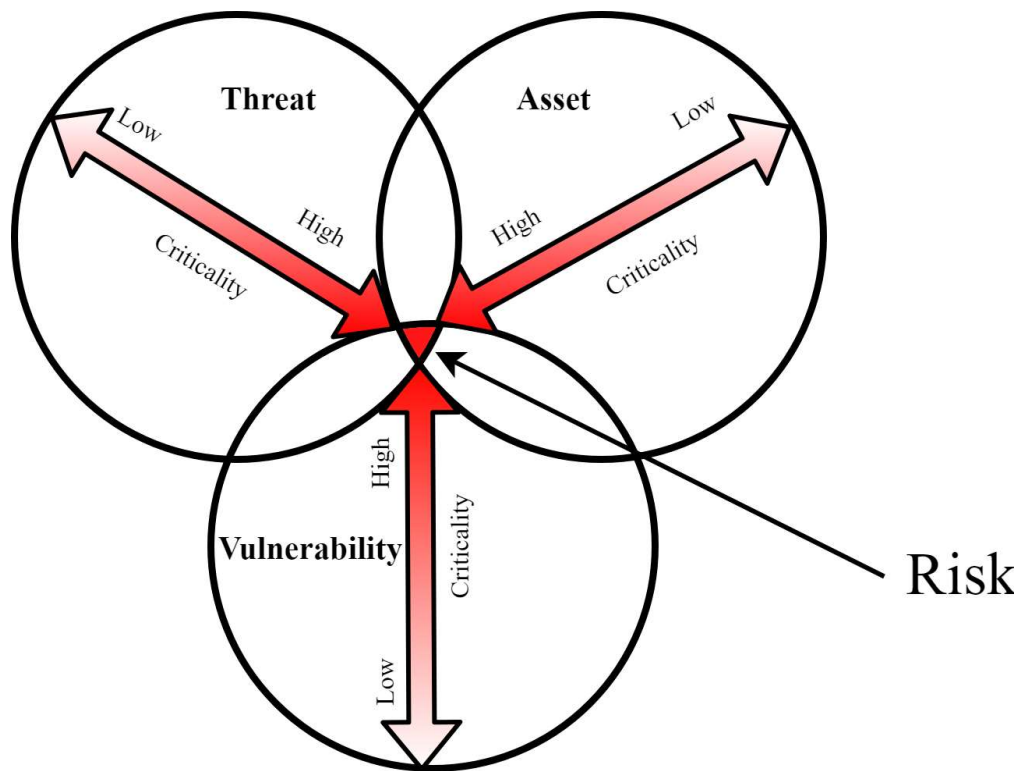
A fundamental concept of information security is the CIA triad. CIA is an abbreviation for confidentiality, integrity and availability, where each of these attributes represent a fundamental objective of information security. These are defined by Andress (2014) as:

- **Confidentiality:** Refers to the ability to protect data from those that are not authorised to view it.
- **Integrity:** Refers to the protection against unauthorised creation, modification or destruction of information.
- **Availability:** Refers to the ability to access the data when it is needed.

By evaluating the elements in the CIA triad in relation to a specific asset in an organisation, the value of this specific asset can be assessed. As explained in the introduction to [Section 3](#), the main goal of information security is to secure the business against threats and ensure success in daily operations by ensuring confidentiality, integrity and availability. A method for evaluating the components of the CIA triad will be demonstrated in [Section 3.4.2](#).

### 3.2 Threat, asset and vulnerability

Assessing risk in information security is usually done with the basis on the three factors threat, asset and vulnerability. This perspective on risk is often called the three-factor approach. Risk is considered as a function of the three factors, as illustrated in Figure 2.



**Figure 2 - Three-factor approach**

To understand the relationship between these factors, they will first be defined in line with the ISO definitions (International Organization for Standardization, 2017):

- Threat: “potential cause of an unwanted incident, which may result in harm to a system or *organization*.”
- Asset: “An asset is anything that has value to the organization and which therefore requires protection.”
- Vulnerability: “weakness of an asset or *control* that can be exploited by one or more *threats*.”

In essence, a threat is what the organisation wants to protect against, and the asset is what the organisation wants to protect. A vulnerability can be thought of as a weakness or hole in the defence. According to this approach, risk level moves in relation to these three factors. As Figure 2 illustrates, the risk level is characterised as “high” if there is a threat with a high strength, the organisation has a highly valuable asset and there is a critical weakness in the defence system.



### 3.3 Frameworks and standards for risk management and information security

There are many different methods available for risk management and risk assessment of information security. The purpose of this section is to inform the reader of some of the available methods that are currently in use and are widely referred to in different industries.

ISO 31000 – provides principles and generic guidelines on risk management. It is not specific to any industry or sector but is intended to contribute principles and general guidelines on how to undertake risk management at the corporate level. This standard is listed because it is a recognised standard that has strongly impacted the risk assessment and risk management field, and is the foundation for several methods, such as the IRAM<sub>2</sub> information risk methodology and COSO enterprise risk management framework.

ISO 27001 – provides requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organisation (International Organization for Standardization, 2013). Builds on the principles presented in ISO 31000.

ISO 27005 – provides guidelines for information security risk management. These guidelines are based on the more generic guidelines of ISO 31000. It supports the general concepts in ISO 27001 on requirements for information security management systems, and is designed to assist the satisfactory implementation of information security based on a risk management approach. (Refsdal, Solhaug, & Stølen, 2015, p. 6).

The FAIR approach – a flexible methodology for assessing information risks. One of the few methods that makes use of quantitative estimates regarding the probability of occurrence of threats.

COSO ERM (2017) – defines essential enterprise risk management components, discusses important principles and concepts for ERM, and provides guidance on enterprise risk management (The Committee of Sponsoring Organizations of the Treadway Commission, 2018).

Information Risk Assessment Methodology 2 (IRAM<sub>2</sub>) (Information Security Forum, 2017) – recognised methodology designed to help organisations understand and manage their information risks. IRAM<sub>2</sub> is based on a qualitative risk assessment approach. It has been decided to use the methodology as a case study for this report, as it is considered within the industry to be best practice despite having several weaknesses according to risk practitioner S. Sviggum, director at PwC (personal communication, April 5, 2018).

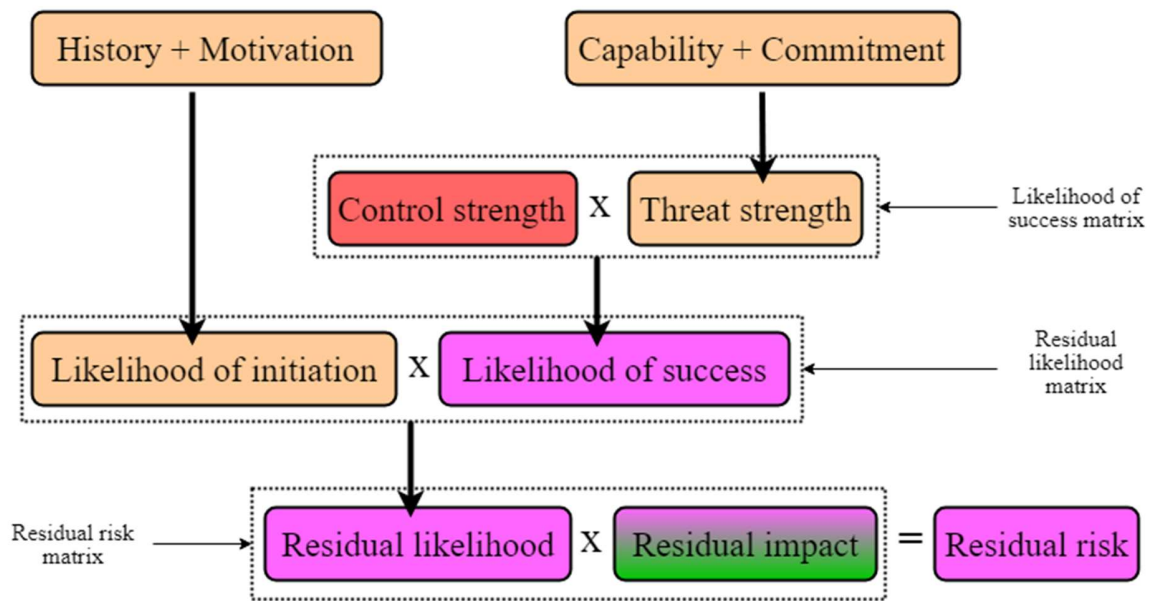
### 3.4 IRAM<sub>2</sub> methodology

Information Risk Assessment Methodology 2 (IRAM<sub>2</sub>) (Information Security Forum, 2017) attempts to combine traditional information risk assessments with enterprise risk management reporting. As explained in [Section 3.2](#), information risks are often assessed in terms of threats, assets and vulnerabilities. This concept is also used in IRAM<sub>2</sub> which is a recognised methodology designed to help organisations understand and manage their information risks. Figure 3 illustrates that the input in IRAM<sub>2</sub> has basis on the three-factor approach that was introduced in [Section 3.2](#).



**Figure 3 – IRAM<sub>2</sub> assesses information risk**

In accordance with IRAM<sub>2</sub>, each threat is assessed using an information risk equation that outputs the corresponding residual risk. Figure 4 shows the key components that form each information risk equation. For every threat established throughout the process there is one information risk equation. This figure is based specifically on adversarial threats, but the process for other threat categories, such as accidental and environmental, follow the same procedure. The only difference lies in which threat attributes are used to derive the likelihood of initiation and the threat strength. In-depth explanations will follow in sections 4.1-4.5.



**Figure 4 - Flowchart IRAM<sub>2</sub> methodology**

Dotted squares in Figure 4 indicates that risk matrices attached to IRAM<sub>2</sub> must be used to derive the resultant of the respective components.

The process of assessing risk within IRAM<sub>2</sub> is done through several phases. The colour in the squares corresponds to the associated phase where the component is derived. More than one colour within a square indicates that the component is derived from more than one phase. The phase and colour combinations, which correspond to IRAM<sub>2</sub>, are as follows:

- Phase B: Green
- Phase C: Orange
- Phase D: Red
- Phase E: Purple.

The information in this section is based on IRAM<sub>2</sub> unless otherwise stated. The methodology will be presented with a walk-through from Phase A: Scoping to Phase E: Risk Evaluation. The methodology is applied to a case study to aid the reader in understanding each step in the process. The case will be to assess the risk regarding the author's master thesis.

The last phase in IRAM<sub>2</sub>, Phase: F: Risk Treatment is not included. Risk treatment is about planning, implementing, and managing appropriate countermeasures, which is outside the scope of this report.

### 3.4.1 Phase A: Scoping

The goal of this phase is to develop a profile of the environment and establish the scope for the assessment. The environment in this instance would be the author's laptop, firewall,

Chromecast, and smart TV. The scope for this analysis will be the master thesis which can be accessed from the laptop.

### 3.4.2 Phase B: Business Impact Assessment

This phase begins with the identification of information assets and assessment of the business impact. In IRAM<sub>2</sub>, information assets are defined as:

“Information assets are information (either physical or logical) that have value to an organisation.”

Relevant information assets will be assets such as the master thesis, private documents, and confidential documents from past projects. In this case, the object of analysis has already been established in Phase A, which is the master thesis.

Once this has been decided, the next step involves assessment of common types of business impacts that the author could encounter because of the loss of one, or more, of the information attributes confidentiality, integrity and availability. These attributes are defined as:

- Confidentiality: the information is accessible only to authorised individuals
- Integrity: the information is accurate (i.e. uncorrupted and unaltered)
- Availability: the information is accessible and usable when required

IRAM<sub>2</sub> recommends each organisation to create their own customised Business Impact Reference Table (BIRT), to best reflect the relevant impact categories and aid the practitioner in determining the impact rating for each category. The scoring levels are negligible (0), low (1), moderate (2) and high (3). Table 2 is an example BIRT for the current case.

Impact rating				
Impact category	Negligible	Low	Moderate	High
<b>Financial</b>	Small loss of <5k NOK	Minor financial loss (<50k NOK)	Moderate financial loss (<150k NOK)	Significant losses (>150k NOK)
<b>Reputational</b>	Negligible impact on reputation	- Low levels of short-term negative responses from supervisors - Minor loss of confidence from supervisors	-Moderate levels of sustained negative responses from supervisors -Moderate loss of confidence	-Significant levels of sustained negative responses from supervisors -Significant loss of confidence

**Table 2 - Business Impact Reference Table (BIRT)**

When assessing business impact in this phase it is the inherent impact, i.e. the potential impact before mitigating controls that are considered. In IRAM<sub>2</sub>, both realistic and worst-case inherent business impact is considered by asking two questions respectively: “What is the most reasonable inherent impact?” and “What is the plausible worst-case inherent impact?”

Some key assumptions related to each information attribute must be agreed on, and then realistic and worst-case inherent impact ratings can begin. Table 3 is an example of impact scenario assumptions specifically for this case.

<b>Information attribute</b>	<b>Assumption type</b>	<b>Descriptions</b>
<b>Confidentiality</b>	Sensitivity	Data can be sensitive and contain confidential information from PwC.
	Volume	How many files have been disclosed, in both the realistic and worst-case scenarios? Realistic: 1-2 files, worst-case: 10 files.
<b>Integrity</b>	Source of truth	The master thesis file is the original file, but with some older versions available elsewhere. Loss of integrity could lead to days or weeks of set-back.
	Volume	
	Decision making	Not applicable
<b>Availability</b>	Timeline	Realistic duration of the asset being unavailable: 1 day. Worst-case: 1 week.

**Table 3 - Impact scenario assumptions**

The information attributes must be assessed for each applicable impact category in the BIRT. IRAM<sub>2</sub> suggests recording the outcomes in a business impact assessment template as in Table 4. Only financial and reputational impacts are assessed in this example. In reality, all relevant impact categories (e.g. operational, legal and regulatory compliance, health and safety) would be assessed.

Information asset	Confidentiality	Integrity	Availability
Master thesis	Overall impact: Realistic: High Worst-case: High	Overall impact: Realistic: Low Worst-case: Moderate	Overall impact: Realistic: Negligible Worst-case: Moderate
	Financial impact: Realistic: High Worst-case: High	Financial impact: Realistic: Negligible Worst-case: Low	Financial impact: Realistic: Negligible Worst-case: Moderate
	Reputational impact: Realistic: Low Worst-case: Moderate	Reputational impact: Realistic: Low Worst-case: Moderate	Reputational impact: Realistic: Negligible Worst-case: Low

**Table 4 - Business impact assessment template**

### 3.4.3 Phase C: Threat Profiling

This phase starts with the identification and prioritisation of relevant threats to the environment. IRAM<sub>2</sub> defines a threat as:

“A threat is anything that is capable, by its action or inaction, of causing harm to an information asset.”

IRAM<sub>2</sub> groups threats by specific threat attributes, which will help the practitioner in understanding the nature of the threat. The threat attribute “intent” is the first grouping usually performed, which results in three groups:

1. Adversarial: threats that perform deliberate actions against the organisation’s information systems or assets, with the goal of causing harm.
2. Accidental: threats that are a result of error or unintentional action that cause harm to the organisation’s information systems or assets.
3. Environmental: threats that are outside the control of the organisation that cause harm to the information systems or assets (e.g. natural hazards).

The first step is to create a threat landscape for the organisation, which is done by identifying the relevant threats and listing them in a common threat list (CTL). IRAM<sub>2</sub> provides the practitioner with a pre-populated list of typical threats that are already grouped into adversarial, accidental and environmental. Table 5 is a common threat list created for this case. For the sake of simplicity only two threats will be considered relevant, and they are highlighted in the table.

<b>Adversarial</b>		<b>Accidental</b>		<b>Environmental</b>	
<b>Threat</b>	<b>Origin</b>	<b>Threat</b>	<b>Origin</b>	<b>Threat</b>	<b>Origin</b>
<b>Hacking group</b>	<b>External</b>	Customer	External	Earthquake	External
<b>Individual hacker</b>	<b>External</b>	Employee	Internal	Fire	Internal/External
<b>Competitor</b>	External	...	...	...	...
<b>Nation state</b>	External	..	..	...	...
<b>Terrorist group</b>	External	.	.	..	..
...	...			.	.

**Table 5 - Common threat list (CTL)**

Once this is completed, the next step involves profiling each threat. This is done by assessing each threat attribute associated with the corresponding threat, e.g. threat attributes history, motivation, capability and commitment are assessed for the adversarial group. This assessment is done by rating each threat attribute from negligible (0), to low (1), moderate (2), or high (3). The goal is to be able to calculate two key risk factors: Likelihood of initiation (LoI) and Threat strength (TS).

LoI is defined as:

“The likelihood that a particular threat will initiate one or more threat events against the environment being assessed”

TS is defined as:

“How effectively a particular threat can initiate and/or execute threat events against the environment being assessed.”

Each organisation should customise their own threat profiling reference tables (TPRT) to provide guidance in this process. Table 6 is an example of such a table that is reproduced from IRAM<sub>2</sub> that addresses the threat attributes for the threats “hacking group” and “individual hacker”.

Threat attribute	Rating			
	Negligible (0)	Low (1)	Moderate (2)	High (3)
<b>History</b>	The threat is not known to have initiated any threat events (e.g. reconnaissance, exploitation/gaining access, exfiltration) relating to the environment over the last 12 months.	The threat is known to have initiated a low number of (often similar) threat events (e.g. reconnaissance, exploitation/gaining access, exfiltration) relating to the environment the last 12 months.	The threat is known to have initiated multiple threat events (e.g. reconnaissance, exploitation/gaining access, exfiltration) relating to the environment the last 12 months.	The threat is known to have initiated multiple and varied threat events (e.g. reconnaissance, physical attack, gaining unauthorised access and theft of information) relating to the environment over the last 12 months.
<b>Motivation</b>	<ul style="list-style-type: none"> <li>-The threat is not expected to initiate a threat event against the environment.</li> <li>-The environment is considered to have limited to no value to the threat because the organisation does not align with any known motivation for the threat.</li> </ul>	<ul style="list-style-type: none"> <li>-The threat is unlikely to initiate a threat event against the environment.</li> <li>-The environment is of minimal value to the threat because the organisation is likely not to align with a known motivation for the threat.</li> </ul>	<ul style="list-style-type: none"> <li>-The threat is likely to initiate a threat event against the environment.</li> <li>-The environment is of moderate value to the threat, because the organisation aligns with known motivations for the threat.</li> </ul>	<ul style="list-style-type: none"> <li>-The threat is highly motivated to initiate a threat event against the environment.</li> <li>-The environment is of significantly high value to the threat, because it closely aligns with more than one known motivations for the threat.</li> </ul>
<b>Capability</b>	<ul style="list-style-type: none"> <li>The threat is characterised as:</li> <li>-involving a single individual</li> <li>-inexperienced and/or unskilled</li> <li>-receiving no external support (e.g. no provision of funding, technology, infrastructure or facilities)</li> <li>-having no access to the environment.</li> </ul>	<ul style="list-style-type: none"> <li>The threat is characterised as:</li> <li>-involving a low number of individuals</li> <li>-having a limited level of experience and skill</li> <li>-receiving limited external support</li> <li>-having limited access to the environment.</li> </ul>	<ul style="list-style-type: none"> <li>The threat is characterised as:</li> <li>-involving many individuals (i.e. a small group)</li> <li>-having a significant level of experience and skill</li> <li>-receiving external support</li> <li>-having a moderate (i.e. general) range of access to the environment.</li> </ul>	<ul style="list-style-type: none"> <li>The threat is characterised as:</li> <li>-involving one or more large groups (often based in multiple locations)</li> <li>-having an extremely high level of experience and skill (i.e. experts)</li> <li>-receiving significant external support</li> <li>-having significant (i.e. privileged) access to the environment.</li> </ul>



<b>Commitment</b>	The threat is not believed to be committing any significant resources to initiating a threat event against the environment being assessed. Any interaction with the organisation or environment being assessed would be considered an opportunity (e.g. visiting a compromised website or activation of malware).	The threat is believed to be committing a small amount of resources to initiating threat events against the environment being assessed. Example: level of commitment may be where a threat expends approximately 25% of its effort and/or computing/network resources initiating threat events, over a limited period (e.g. from days to weeks).	The threat is believed to be expending a moderate amount of resources to initiating threat events against the environment being assessed. Example: level of commitment might be where the threat expends at least 50% of its effort and/or computing/network resources initiating threat events against the organisation's infor. systems being assessed, for a significant period (e.g. from weeks to months).	The threat is believed to be expending most, if not all, resources to initiating threat events against the environment being assessed. Example: level of commitment might be where the threat is willing to initiate and sustain an advanced persistent threat (APT) against a target. This would require a significant level of effort (i.e. close to 100% of their activities and/or computing/network capacity) over a long period of time (e.g. from months to years).
-------------------	---	--	---	--

**Table 6 - Threat Profiling Reference Table (TPRT)**

When all relevant threat attributes associated with a specific threat have been assessed, it is recommended to record the results in a threat profiling template. Table 7 shows how this can be presented for the threats “hacker group” in the first row, and “individual hacker” in the second row.

<b>History rating</b>	<b>History rationale</b>	<b>Motivation rating</b>	<b>Motivation rationale</b>	<b>Capability rating</b>	<b>Capability rationale</b>	<b>Commitment rating</b>	<b>Commitment rationale</b>
Negligible (0)	The threat is not known to have initiated any threat events relating to the environment over the last 12 months.	Low (1)	-Threat is unlikely to initiate a threat event against the environment. -The environment is of min. value to the threat because the organisation is likely not to align with a known motivation for the threat.	Low (1)	The threat is characterised as: involving a low number of individuals, having a limited level of experience and skill.	Negligible (0)	The threat is not believed to be committing any significant resources to initiating a threat event against the environment being assessed. Any interaction with the organisation or environment being assessed would be considered an opportunity.
Low (1)	The threat is known to have initiated a low number of threat events relating to the environment the last 12 months.	Low (1)	-Threat is unlikely to initiate a threat event against the environment. -The environment is of min. value to the threat because the organisation is likely not to align with a known motivation for the threat.	Negligible (0)	The threat is characterised as: involving a single individual, inexperienced and/or unskilled, receiving no external support.	Low (1)	The threat is believed to be committing a small amount of resources to initiating threat events against the environment being assessed. An example of this level of commitment may be where a threat expends approx. 25% of its effort.

**Table 7 - Threat profiling template**

This must be done for every threat within the threat landscape. Once this has been carried out, Likelihood of initiation (LoI) and Threat strength (TS) can be determined. LoI is derived by

summing the scores from the history rating and motivation rating. TS is derived by summing the scores from the capability rating and the commitment rating. The resulting LoI and TS for the threats “hacking group” and “individual hacker” become, respectively:

$$LoI = History + Motivation = Negligible (0) + Low (1) = Low (1)$$

$$TS = Capability + Commitment = Low (1) + Negligible (0) = Low (1)$$

and

$$LoI = History + Motivation = Low (1) + Low (1) = Low (2)$$

$$TS = Capability + Commitment = Negligible (0) + Low (1) = Low (1)$$

IRAM<sub>2</sub> provides risk factor scoring and reference tables where the practitioner can determine the different scores.

When all the threats are profiled, a prioritised threat landscape should be created. According to IRAM<sub>2</sub>, this can be sorted by either listing the highest LoI score first, or TS score. Table 8 is an example of a prioritised threat landscape with the actual scores from the two highlighted rows and some hypothetical scores greyed out to show the setup.

Threat	Threat group	Origin	Likelihood of Initiation	Threat strength	Threat priority rating
Terrorist group	Adversarial	External	Moderate (4)	High (5)	1
Individual hacker	Adversarial	External	Low (2)	Low (1)	2
Hacking group	Adversarial	External	Low (1)	Low (1)	3
Fire	Environmental	Internal	Low (0)	Low (0)	4
Nation state	Adversarial	External	Low (0)	Low (0)	5
...	...	...	...	...	6
..	..	..	..	..	7

**Table 8 - Prioritised threat landscape**

The next step is to figure out which threat event is associated to each threat. IRAM<sub>2</sub> makes it clear that the process of finding threat events and determining if they should be in scope is a subjective process that relies on the knowledge of the persons involved. The methodology comes with a Threat Event Catalogue (TEC) which lists threat events that threats in each threat group could initiate. The initiation requirements for adversarial threats are:

- Origin (i.e. internal or external); “some threat events can only be executed by organisational insiders such as employees with physical and logical access to organisational information systems”.
- Threat strength; “certain threat events require more capability (Adversarial threat events) or privilege (Accidental threat events) to effectively initiate (e.g. creating and utilising zero-day malware or executing an unintentional change in a production environment). This is defined as ‘minimum threat strength required to initiate threat event’ in the TEC.”

Mapping threat events to each threat is done by working through the prioritised threat landscape from the highest priority rating to the lowest. The highest threat priority rating in this case comes from the threat “individual hacker”, which belongs to the threat group adversarial, where origin is external, and has a threat strength of low. Using the TEC, the practitioner looks for each threat event that meets these requirements. Table 9 is an excerpt of the TEC with some highlighted threat events to show that these fulfil the initiation requirements and can thus be mapped to the threat.

<b>Threat event ID</b>	<b>Threat event</b>	<b>Threat group</b>	<b>Origin</b>	<b>Min. threat strength</b>
ADV005	Conduct a DoS attack	Adversarial	External	Moderate
<b>ADV007</b>	<b>Introduce malware to information system</b>	<b>Adversarial</b>	<b>External</b>	<b>Low</b>
ADV014	Theft of information system hardware	Adversarial	Internal	Low
<b>ADV016</b>	<b>Unauthorised network scanning</b>	<b>Adversarial</b>	<b>External</b>	<b>Negligible</b>

**Table 9 - Threat event catalogue (TEC) (excerpt)**

Once a threat event has been mapped to a specific threat in the prioritised threat landscape, there is no need to check if the same threat event can be mapped to lower rated threats in the prioritised threat landscape.

The last step in this phase is to decide which information asset each threat event could impact. However, IRAM<sub>2</sub> suggests first to identify which process or technology component(s) could be impacted by the threat event, and then determine which information assets that are related to those components. The last activity in this step is to determine the highest realistic and worst-case inherent business impact rating for each component. This forms the basis for each information risk equation. Since the scope of this case is on one specific information asset, all components that are identified will be associated to that same information asset. Table 10 is an

example, but this should be done for each unique combination of threat, threat event, and impacted information asset.

		Highest assessed realistic and worst-case inherent business impact rating			
Threat	Threat event	Component	Confidentiality	Integrity	Availability
Individual hacker	Introduce malware	Dropbox	Realistic: Moderate Worst-case: High	Realistic: Low Worst-case: Moderate	Realistic: Negligible Worst-case: Moderate
Individual hacker	Introduce malware	Laptop	Negligible	Negligible	Negligible

**Table 10 - Determining the basis for each information risk equation**

#### 3.4.4 Phase D: Vulnerability Assessment

Phase D consists of assessing how vulnerable the information assets are to each in-scope threat event. This step involves:

- Choosing controls that are relevant to the environment being assessed. A control is defined as a measure that is modifying risk (ISO (2017)).
- Mapping the controls to in-scope threat events and decide on their relevance
- Assess the implementation of controls
- Determine control strength for each combination of threat event and component.

Every organisation should have a control library, which is an overview of an organisation’s controls, that provides support to the management of information security. In IRAM<sub>2</sub>, several potential sources to such control libraries are listed:

- The ISF Standard of Good Practice for Information Security
- ISO/IEC 27002:2013
- NIST Cybersecurity Framework
- Payment Card Industry Data Security Standard (PCI DSS)

In IRAM<sub>2</sub>, a vulnerability is defined as:

“A vulnerability is a weakness in people, process or technology in an environment, which could be exploited by one or more threats.”

Vulnerability and threat strength are used to estimate the likelihood that a threat event is successful. This is called the Likelihood of Success (LoS).

To assess vulnerability, two concepts are used:

- **Relevance:** “The extent to which a control can reduce the likelihood and/or impact from a threat event.”
- **Implementation:** “The extent to which a control is implemented within the environment being assessed.”

Controls that are applicable for the environment being assessed in this case can be e.g.:

- Control 1: Firewall firmware should be updated regularly.
- Control 2: Antivirus software should be installed on laptop.
- Control 3: Dropbox password should be considered strong.

The next step is to rate the relevance of these controls to the threat events, by the aid of a scoring system as shown in Table 11:

Score	Means	Extent of relevance	Guidance
4	Extent to which a control can reduce the likelihood and/or impact of a threat event	Fully relevant	The control can reduce the likelihood and/or impact of a threat event in 96-100% of cases
3		Mostly relevant	The control can reduce the likelihood and/or impact of a threat event in 66-95% of cases
2		Moderately relevant	The control can reduce the likelihood and/or impact of a threat event in 36-65% of cases
1		Partially relevant	The control can reduce the likelihood and/or impact of a threat event in 6-35% of cases
0		Not relevant	The control can reduce the likelihood and/or impact of a threat event in 0-5% of cases

**Table 11 - The extent of control relevance**

This should then be recorded in a control relevance table, see Table 12:

	<b>Threat event:</b>	<b>ADV007</b>	<b>ADV016</b>
<b>Control number</b>	<b>Control description</b>	<b>Introduce malware to information systems</b>	<b>Unauthorised network scanning</b>
<b>1</b>	Firewall firmware should be updated regularly	4	4
<b>2</b>	Antivirus software should be installed on laptop	3	2
<b>3</b>	Dropbox password should be considered strong	0	0

**Table 12 - Control relevance table**

Next, the practitioner is to assess the control implementation in the environment. In IRAM<sub>2</sub>, the scoring system used for this step is as shown in Table 13.

<b>Score</b>	<b>Means</b>		<b>Guidance</b>
<b>4</b>	Extent to which a control is implemented	In all cases (or "Yes")	96-100%
<b>3</b>		In most cases	66-95%
<b>2</b>		In about half the cases	36-65%
<b>1</b>		In a few cases	6-35%
<b>0</b>	Not implemented	In no cases (or "No")	0-5%

**Table 13 - Extent of implementation of control**

This should be recorded in a control implementation assessment table, see Table 14:

Control statement	Control implementation score	Control implementation rationale	Reference to evidence documents
Firewall should be updated regularly	0	The firewall has never been updated, at least manually	N/A
Antivirus software should be installed on laptop	3	Antivirus is installed, but it is a free version	N/A
Dropbox password should be considered strong	4	Password is 30 ch. with 181 bits quality	N/A

**Table 14 - Control implementation assessment**

The last step is to calculate the control strength (CS) score for each combination of threat event and component by using the following formula:

$$CS = \frac{\sum_{j=1}^n r_j i_j}{\sum_{j=1}^n r_j}$$

where

$r_j$  = control relevance score for control number  $j$

$i_j$  = control implementation score for control number  $j$

In this case,

$$CS = \frac{\sum_{j=1}^3 r_j i_j}{\sum_{j=1}^3 r_j} = \frac{r_1 i_1 + r_2 i_2 + r_3 i_3}{r_1 + r_2 + r_3} = \frac{4 * 0 + 3 * 3 + 0 * 4}{4 + 3 + 0} \cong 1,3$$

This is a dimensionless quantity. Using the risk factor scoring and reference tables provided in IRAM<sub>2</sub> in Appendix H, the control strength score 1,3 can be found in the interval for control rating equal to “Low”.

### 3.4.5 Phase E: Risk Evaluation

The risk evaluation phase consists of evaluating the remaining risk factors (likelihood of success, residual likelihood, and residual business impact rating) and derivation of the residual risk rating for each risk. These risks are determined using matrices provided in Appendix H: Risk factor scoring, and reference tables found in IRAM<sub>2</sub>.



As preparation for this phase, it is recommended to create a table showing all threats with the corresponding risk factors determined in earlier phases. This forms the setup for the information risk equation. For the highest priority threat in this case recorded in such a table, see Table 15:

Threat (highest priority)	Likelihood of initiation	Threat strength	Threat event	Impacted assets and/or component(s)	Control strength	Likelihood of success	Residual likelihood	Residual impact rating	Inherent business impact ratings	Residual risk rating
Individual hacker	Low	Low	Introduce malware to information system	Master thesis, Dropbox	Low	Derived during this phase	Derived during this phase	Derived during this phase	<b>Highest overall impact scenarios:</b> Realistic: Moderate Worst-case: High  Confidentiality: Realistic: Moderate (Financial) Worst-case: High (Financial)  Integrity: Realistic: Low (Reputational) Worst-case: Moderate (Reputational)  Availability: Realistic: Negligible (Financial/Reputational) Worst-case: Moderate (Financial)	Derived during this phase

**Table 15 - Recorded information risk equation**

IRAM<sub>2</sub> defines likelihood of success (LoS) as:

“The likelihood that the strength of a threat will be sufficient to overwhelm the strength of controls in place (or planned), resulting in a successful threat event”

The LoS matrix, see Table 16, gives LoS = Low (since threat strength is low and control strength is low for the threat “individual hacker”).

		Threat strength			
		Negligible	Low	Moderate	High
Control strength	High	Negligible	Negligible	Low	Moderate
	Moderate	Negligible	Low	Moderate	High
	Low	Low	Low	High	High
	Negligible	Low	Moderate	High	High

**Table 16 - Likelihood of success (LoS) matrix**

This must be derived for all relevant threats and associated threat event and component combinations that were derived in earlier phases.

Next, the practitioner should derive the residual likelihood for each threat by using the residual likelihood matrix, see table Table 17:

		Likelihood of success			
		Negligible	Low	Moderate	High
Likelihood of initiation	High	Moderate	Moderate	High	High
	Moderate	Low	Moderate	Moderate	High
	Low	Low	Low	Moderate	Moderate
	Negligible	Negligible	Low	Low	Low

**Table 17 - Residual likelihood matrix**

From the previous step, likelihood of success is low. Likelihood of initiation, found in Table 15, is low. The resulting residual likelihood is then derived to be low.

The next step is to determine the residual business impact rating, which is defined as:

“The residual business impact rating is the business impact rating after the relevant (i.e. realistic or worst-case) impact scenario have been determined, and the effect of controls in place (or planned) has been assessed.”

This rating is found by first selecting a suitable inherent impact scenario for each risk, i.e. either realistic or worst-case. The recommended default starting point is to start with the realistic inherent impact scenario, which in this case is moderate (see Table 15). Deciding which is suitable (realistic or worst-case) demands knowledge regarding threat strength and control strength ratings. In this case both threat strength and control strength are low. Based on this it is judged that the appropriate residual business impact scenario should stay at moderate. Second

step is to consider if any of the relevant controls aid in the reduction of inherent impact ratings for confidentiality, integrity and availability. Lastly, overall residual impact rating must be set for each risk to the highest of the residual impact ratings.

Next step is to derive the residual risk rating. This is done by using a residual risk rating matrix, see Table 18:

		Residual impact			
		Negligible	Low	Moderate	High
Residual likelihood	High	Moderate	Moderate	High	High
	Moderate	Low	Moderate	Moderate	High
	Low	Low	Low	Moderate	Moderate
	Negligible	Negligible	Low	Low	Low

**Table 18 - Residual risk rating matrix**

The residual risk rating for the case applied, with residual likelihood being rated low and residual impact rated moderate, result in a residual risk rating of moderate for this specific risk.

When the residual risk rating for all the risks in the environment have been assessed, the risks can be inserted into a prioritised residual risk profile, which completes Phase E. The final phase, which is scoped out of this report, involves determining the appropriate risk treatment for each of the risks found.

## 4 Evaluation of IRAM<sub>2</sub>

Evaluation of IRAM<sub>2</sub> will be partly based on the generic guidelines on risk management provided in ISO 31000 (International Organization for Standardization, 2018). This is a recognised standard that has strongly impacted the risk assessment and risk management field. The standard has received criticism (e.g. (Aven, 2011c)) for aspects such as being unclear on fundamental concepts, risk and probabilities. However, there is still broad agreement that the standard builds on good principles and follows a logical process. It is on these points the methodology will be evaluated.

Furthermore, there are other aspects of the methodology that will be discussed (e.g. risk conceptualisations, calculation methods, use of matrices and background knowledge). These aspects will be discussed in Sections 4.1 and 4.3, and will be based on existing scientific literature on risk and guideline documents (e.g. (SRA, 2015)).

The structure of this section follows a top-down approach covering the conceptual level of IRAM<sub>2</sub> first, and then discussing the principles and the process. Following this, the methods used in the methodology will be discussed.

### 4.1 Concepts

IRAM<sub>2</sub> is built on several concepts, and many are well-defined, precise and unambiguous. A few of the concepts, however, are debatable and some of them are argued in scientific literature to be unsuccessful in producing consistent and meaningful definitions (Aven, 2011c). The latter relates to key generic concepts within the field of risk analysis and how they are defined according to the guidelines recommended by the Society for Risk Analysis (2015).

This section does not contain an exhaustive list of all the concepts used in IRAM<sub>2</sub> but will review some of them to demonstrate the varying degree of concept quality. The structure of this section follows a “best to worst” structure.

#### **Information assets and threats**

The two concepts of information assets and threats are examples of well-defined, precise and unambiguous concepts in IRAM<sub>2</sub>.

Information assets is defined as:

“Information assets are information (either physical or logical) that have value to an organisation”

A threat is defined as:

“A threat is anything that is capable, by its action or inaction, of causing harm to an information asset”

The definition of a threat is also listed with a warning commenting on the misuse of this concept in general, and to alert the practitioner on paying attention to how it is defined in IRAM<sub>2</sub>.

### **Realistic and worst-case business impact**

Realistic business impact and worst-case business impact are defined, respectively, as:

“The business impact that is expected to occur in a typical scenario”

“The business impact that could occur in an extreme (i.e. very rare) scenario”

These concepts can be argued to not be well-defined and precise. Evidently, by making the risk practitioner distinguish between the most likely scenario and a very rare scenario will contribute to – at least to some extent – a more precise risk assessment. Yet, it is not clear what a “typical” or “very rare” scenario imply. To make this distinction between realistic and worst-case scenarios more useful, the differences should be more precise. However, in the state the definitions are now, there is some usability.

### **Vulnerability**

As stated by Aven (2015, p. 19), the concept of vulnerability is closely related to risk, and essentially it means risk conditional on the occurrence of an event. A vulnerability is defined in IRAM<sub>2</sub> as:

“A weakness in people, process or technology in an environment, which could be exploited by one or more threats.”

Now, consider one of the overall qualitative definitions of vulnerability in the SRA glossary (2015):

“The degree a system is affected by a risk source or agent”

SRA considers vulnerability as “the degree” of something, while IRAM<sub>2</sub> refers to “a weakness”. However, a vulnerability in IRAM<sub>2</sub> is interpreted similarly as a vulnerability in (SRA, 2015). The vulnerability concept in the methodology is used to determine the likelihood of a threat event being successful, and as such, vulnerability is used as a measure for how vulnerable a system is.

### **Uncertainty**

Risk analysts addressing uncertainty in risk assessments regarding non-intentional acts (e.g. natural disasters, equipment failure on an offshore platform, etc.) are generally well versed in their methods, although that is not always apparent. However, considering uncertainty when there is an intelligent adversary adds a different layer of uncertainty – the behaviour of the adversary (S. Guikema, 2012).

In IRAM<sub>2</sub> (2017, p. 3), the reader is presented with risk fundamentals. After risk is defined (see **Risk** in this section), the risk concept is further decomposed:

“Risk is often expressed as a combination of two key determinants: the likelihood of a certain event occurring (an expression of the ‘uncertainty’ in the definition above) and the impact such an event would have on the achievement of one or more objectives.”

“...the definition above” is referring to the ISO definition of risk (see **Risk** in this section). This statement suggests that the methodology considers only uncertainty related to the likelihood of the event, but not uncertainty tied to the impact. This does not exactly match ISO Guide 73:2009 definition of uncertainty:

“Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.”

It is not stated explicitly that IRAM<sub>2</sub> is using ISO’s definition for uncertainty, but it should be consistency in the concepts that the methodology forms its foundation on.

### **Likelihood/probability**

ISF (2017) defines likelihood as:

“Likelihood is the chance that a threat will initiate a successful threat event within a defined period of time.”

This resembles ISO’s definition of likelihood:

“Chance of something happening”

However, like ISO, ISF does not define what a chance is. Aven argues (Aven, 2011c) that there is a need for a broad interpretation that clearly defines all concepts introduced if it is to be used in a professional risk management context.

### **Risk**

IRAM<sub>2</sub> has adopted the ISO Guide 73:2009 definition of risk. The risk management terminology of ISO has been discussed in (Aven, 2011c) where several weaknesses of the terminology is highlighted. One of them has to do with the definition of risk: “Risk is the effect of uncertainty on objectives”, where “effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats.” (International Organization for Standardization, 2018, p. 1). Aven argues that this definition is not precise enough and can lead to different interpretations depending on who the reader is. The author presents an example to show its ambiguity (Aven, 2011c, p. 2). Here, the example is reproduced with some adjustments applied to information risk to illustrate the point:

The outcome of an activity is either 0 or 1, where 0 refers to no power failure of server. 1 refers to power failure of server. The probabilities are, respectively, 0.1 and 0.9. The expected outcome,  $E(\text{outcome}) = 0.1*0 + 0.9*1 = 0.9$ . Deviation from the expected is either 0 or 1. The outcome is uncertain, and the objective is the outcome 0 (zero power failures). According to

ISO, risk is the “effect of uncertainty”, i.e. an outcome 0 or 1, “on objectives”, i.e. outcome 0 meets the objective although 1 does not.

This can be hard to interpret. One way of interpreting this, according to the article, is that risk is the event that the objective is not met, i.e. risk is the event “power failure of server” (outcome 1). The event is a deviation from the expected; it is subject to uncertainties and relates to the objectives (Aven, 2011c, p. 2). According to this, the situation with a power failure is the risk. This outcome is liable to uncertainties, but the risk concept confines to the event “power failure” – the uncertainties is a separate domain. These definitions lead to conceptual challenges and do not fit well for most purposes (Aven, 2011c, p. 2).

However, as also pointed out in (Aven, 2011c), ISO’s definition of risk incorporates the uncertainty dimension rather than the probability dimension. As mentioned in [Section 2.1](#), probability is only a tool for determining risk level and does not capture potentially important uncertainty aspects that are tied to the probabilities.

## 4.2 Comparison with ISO 31000

In this section, there will firstly be an evaluation of the principles in IRAM<sub>2</sub>. Following that is an evaluation of the process.

### 4.2.1 Principles

According to ISO 31000 (2018), the purpose of risk management is the creation and protection of value. It is stated that the principles provide guidance on the characteristics of effective and efficient risk management, communicating its value and explaining its intention and purpose. The standard lists eight principles, which are:

- a) integrated
- b) structured and comprehensive
- c) customised
- d) inclusive
- e) dynamic
- f) best available information
- g) human and cultural factors
- h) continual improvement

The reader is pointed to the standard for further explanation on each principle. Each of the principles will now be evaluated up against IRAM<sub>2</sub>.

#### **Integrated**

The methodology encourages engagement with stakeholders and management. It emphasizes the need for participation from different stakeholders at various key stages during the process. According to ISO (2018), this is an important step towards effective and efficient risk management.

Prior to implementing IRAM<sub>2</sub>, it is recommended to follow certain requirements listed (see (Information Security Forum, 2017, p. 12)). One of these requirements is to have an organisational risk management framework in place, which should help integrate the methodology into a broader risk management process within an organisation.

The methodology encourages integration with organisational activities such as sharing the same business impact assessment tables as used for other parts of enterprise risk assessments. This should ensure better integration.

### **Structured and comprehensive**

IRAM<sub>2</sub> has a structured approach. Each phase starts with a precise overview of what the phase objectives are and the steps to get there. It also lists the key inputs and outputs for each specific phase.

The methodology has a clear and, for the most part, logical flow for the various activities. However, the placement of Phase B: Business Impact Assessment is worth discussing. Assessment of business impact because of the loss of information attributes involves establishing the consequences of potential threats to the organisation. In IRAM<sub>2</sub>, this is done before the threats and threat events, i.e. the initiating events, are determined. The result of this is a limited analysis which concentrates on a select few events capable of influencing performance measures that are highlighted in the analysis (Aven, 2015, p. 34).

According to Aven (2015), the backward approach demands less time investment. However, substantial experience and capability is required to make sure the analysis provides sufficient basis for decision-making. In IRAM<sub>2</sub>, the placement of the phase is justified by being a natural segue from Phase A: Scoping due to the involvement of the same stakeholders.

It should be noted that a comment in the beginning of Phase B states that the practitioner can decide to assess likelihood of threats and impact components of the information risk equation in their preferred sequence.

### **Customised**

It is encouraged in the methodology to customise the framework to each organisation. ISF (2017) advocates to customise a selection of tables used in the methodology, e.g. an approved;

- Business impact reference table
- Organisational threat landscape
- Organisational threat profiling reference table
- Organisational threat event catalogue
- Control relevance table.

In this sense, IRAM<sub>2</sub> promotes customisation.



### **Inclusive**

The methodology clearly highlights which stakeholder(s) should participate in each phase. This ensures appropriate and timely involvement of stakeholders, which, in line with ISO (2018), enables their knowledge, views and perceptions to be considered.

### **Dynamic**

The ever-increasing rate of digitalisation results in the emergence of information risks, attacks that increase in frequency and in level of sophistication (Oredsson, 2017). The principle of staying dynamic in such a landscape can be argued to be demanding and bordering unachievable. In an attempt to deal with this, however, ISF (2017) recommends the practitioner and key stakeholders to review risks on a regular basis, together with other potential contributing factors in the organisation. Considering new risks, nonetheless, is a tedious and time-consuming process in IRAM<sub>2</sub>.

### **Best available information**

IRAM<sub>2</sub> bases the risk equations on a selection of threat attributes that are rated using a semi-quantitative scoring system. Weighing the history attribute in calculation of adversarial threats can be problematic. From the perspective of this report, best available information regarding input to risk assessment is based on having criteria for the strength of knowledge that lies behind the probabilities, which are missing; there should be made changes in the assessment of likelihood of initiation; and subjective probabilities should be reflected.

### **Human and cultural factors**

It is stated in ISO (2018) that human behaviour and culture heavily influence risk management. Implementation of this principle is essential for assessing threats within information security. This is because understanding human behaviour and culture will aid the risk practitioner in pinpointing e.g. motivation, capability and commitment of potential attackers. A common thread throughout IRAM<sub>2</sub> is that the practitioner is instructed to customise for example the threat profiling reference table for the environment being assessed.

### **Continual improvement**

The ISF recommends piloting the methodology within an organisation, which can help improve understanding through learning and experience. ISF also offers IRAM<sub>2</sub> training and attendance at specific courses. Furthermore, ISF encourages the practitioner to provide feedback, both to ISF and to other members, which can be used to continually improve the methodology.

#### **4.2.2 Process**

The risk management process according to ISO (2018) involves systematic application of policies, procedures and practices to the activities of communicating and consulting,

establishing context and assessing, treating, monitoring, reviewing, recording and reporting risk. This section will follow the process structure in IRAM<sub>2</sub>, rather than the process structure of ISO. This decision was made because one of the phases in IRAM<sub>2</sub> is not as clear as to where it belongs in the ISO equivalent process.

### **Phase A: Scoping**

In Phase A: Scoping of IRAM<sub>2</sub> is the development of an environmental profile, which aids the risk practitioner in understanding the area to be assessed. Further, this phase includes defining and agreeing on the scope for the assessment. This complies with the scope, context, criteria phase in ISO (2018).

### **Phase B: Business Impact Assessment**

Phase B: Business Impact Assessment is not as clear where it should be placed in the ISO equivalent process. This is because the Business Impact Assessment phase identifies information assets, which is a scoping process. In addition to this, the practitioner must also assess the business impact of suffering a loss of one or more of its information attributes (confidentiality, integrity, availability) during this phase. This is part of the risk assessment phase in ISO where consequences and their impact on objectives should be considered. It should be noted that IRAM<sub>2</sub> lists a warning in this phase that the user should not consider cause of impact at this stage.

### **Phase C: Threat Profiling**

Phase C: Threat Profiling is the equivalent to the risk identification step in ISO. According to ISO, the purpose of this step is to identify risks by finding, recognising and describing risks that help or prevent the organisation achieving its objectives. In IRAM<sub>2</sub>, the purpose of this phase is to identify and prioritise relevant threats and decide how they can manifest to cause harm to the environment. However, this phase also includes risk analysis. As stated in the ISO guidelines, the purpose of risk analysis is to comprehend the nature of risk and its characteristics.

### **Phase D: Vulnerability Assessment**

Phase D: Vulnerability Assessment consists of identifying the amount to which the information assets are vulnerable to each in-scope threat event. This also fits in ISO's risk identification and risk analysis steps.

### **Phase E: Risk Evaluation**

Phase E: Risk Evaluation complies reasonably well with risk evaluation in ISO. In IRAM<sub>2</sub>, risk evaluation involves the evaluation of the risk factors (likelihood of success, residual likelihood, and residual business impact rating) and the derivation of the residual risk rating for each risk (Information Security Forum, 2017, p. 45). These risks are then prioritised in a residual risk profile for aiding in decision support.

ISO recommends comparing the results with established risk criteria to determine where additional action is required (International Organization for Standardization, 2018, p. 12). In IRAM<sub>2</sub>, during Phase F: Risk Treatment, there is a Section for determining whether any of the risks identified exceed the organisation's risk appetite. Consider ISF's definition of risk appetite (Information Security Forum, 2017, p. 53):

“Risk appetite is the nature (i.e. risk category) and amount (i.e. risk rating) of risk that an organisation is willing to accept to achieve its objectives.”

This has similarities to the ISO definition of risk criteria (International Organization for Standardization, 2018, p. 10):

“The organization should specify the amount and type of risk that it may or may not take, relative to objectives.”

This suggests that Phase E: Risk Evaluation does not cover all aspects of the risk evaluation step in ISO. It is not judged as a weakness of IRAM<sub>2</sub> to evaluate risk criteria during Phase F rather than in Phase E, it is merely an acknowledgement of a different approach.

### **Phase F: Risk Treatment**

Phase F: Risk Treatment is outside the scope of this report. See Phase E: Risk Evaluation for comments.

## **4.3 Methods**

The order of the issues discussed in this section reflects the importance of them, from the author's point of view.

### **4.3.1 Calculation methods**

IRAM<sub>2</sub> combines the traditional three-factor cyber risk approach with the two-factor approach commonly used in ERM. The basis of the information risk equation in the methodology is a function of likelihood and consequence. Looking at adversarial threats, which is the focus of this report, there are some points to discuss such as the use of the history attribute and the scoring system.

In the information risk equation proposed by ISF (2017), residual likelihood decomposes to threat agent assessments and vulnerability assessments. The consequence dimension uses asset value assessments for scoping purposes and business impact estimates. Recall Figure 5, reproduced from the introduction of [Section 3.4](#):

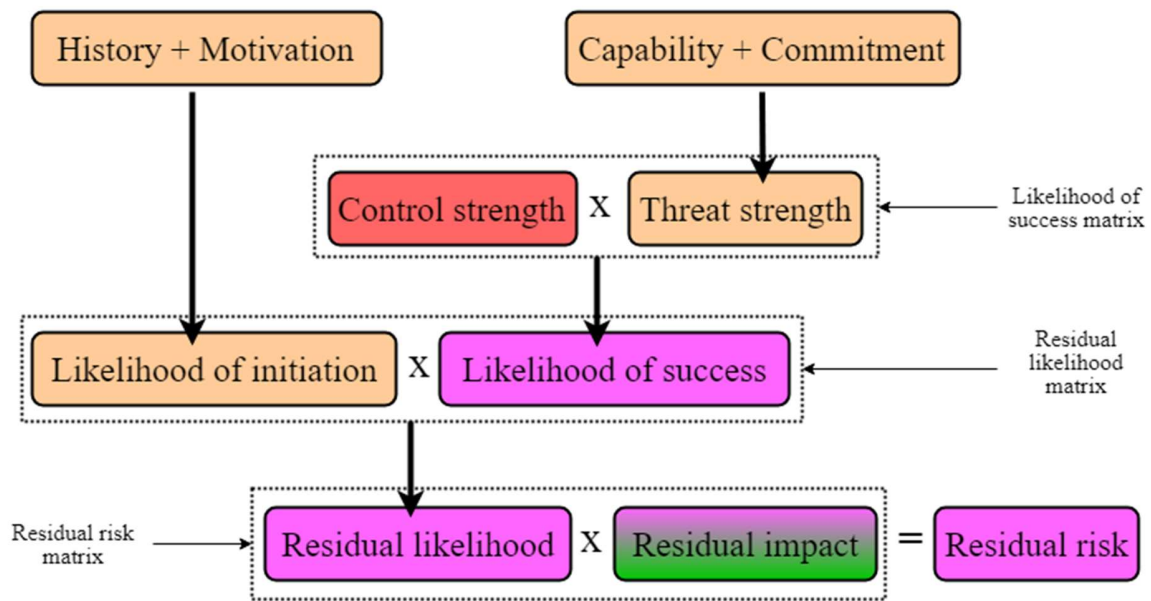


Figure 5 - Flowchart of IRAM2

Further decomposition of the likelihood dimension (residual likelihood) shows that the history attribute is one of the main components for likelihood of initiation. The question can be raised if this attribute should play such a significant role in determining the likelihood of initiation. It can be argued that history does not necessarily have an impact on the likelihood of a future event, yet in IRAM<sub>2</sub>, this attribute is summed with the motivation attribute to give a total score for the likelihood of initiation. Most will agree that the history regarding an event can be an important source of information to determine future risk. This claim is not disputed. As Aven (2011a) points out, historical data provide insights into risk. If it is presumed that the future will be as history shows, good predictions regarding the future could be obtained. However, incorporating history as one of the main components to determine the risk of adversarial threats is problematic. The ramification of this will be discussed below.

The rating system in IRAM<sub>2</sub> is based on qualitative judgements that determine the risk factor score for each threat. Each of the threat attributes are assigned a rating of negligible, low, moderate or high, where each rating has a score from 0-3, respectively. The risk factor “Likelihood of initiation” consists of the threat attributes history and motivation, and the scores of these are added to generate the score of likelihood of initiation. Summing the attributes seems arbitrary and can be argued does not give a justified picture of the likelihood of an initiating event. An example will illustrate this:

If a threat actor emerges with a high motivation for an attack, but no relevant history from this actor exists, the likelihood of initiation can never reach a score higher than a three out of a total score of six. Restriction on getting a higher score just because there is no history, is hard to justify. Intuitively, it is easy to see how the likelihood of initiation could be considered high for

a given threat based on just motivation, despite no existing history (known to the assessor) of such a threat actor. This is especially relevant in the world of an ever-evolving cyber risk landscape where threat actors are constantly finding new ways of exploiting its target. Treating the history attribute as one of the main components for likelihood of initiation can lead to underestimating or missing critical threats.

It should also be noted the history attribute is to be rated as a frequency. For example, the rating “high” for the history threat attribute is characterised as:

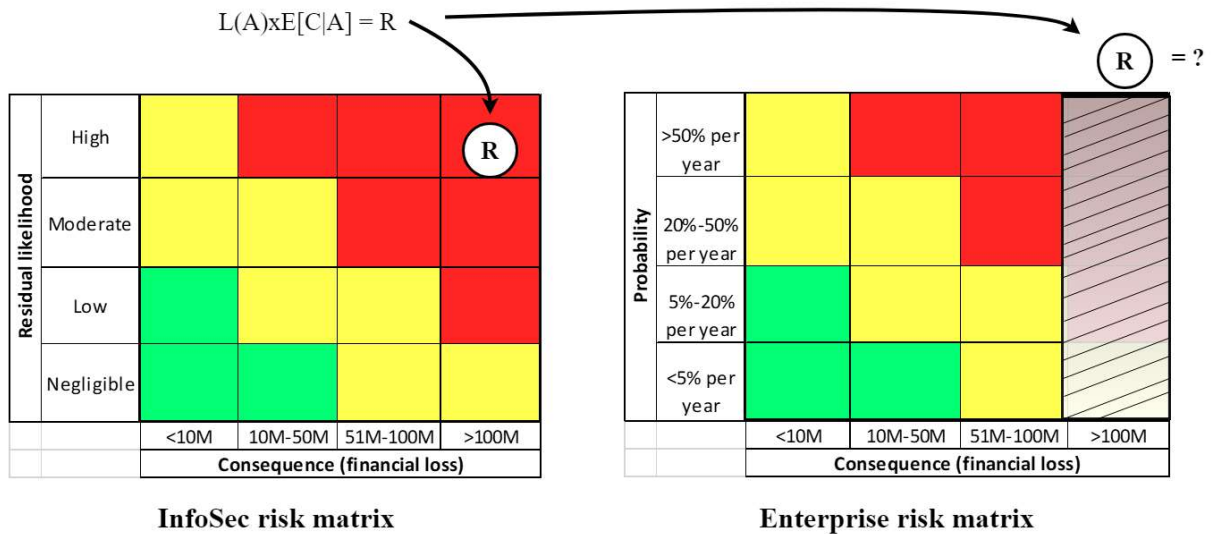
“The threat is known to have initiated multiple and varied threat events...relating to the environment over a predefined period of time (e.g. the previous 12 months).”

In the current risk scoring system, it is reasonable that rating the history threat attribute is based on the frequency of occurrence. A logical train of thought when considering a potential threat event would be to ask, “Has this happened before?” If yes, “how many times has this event occurred in the past e.g. year”. On the other hand, the threat attributes capability, motivation and commitment are not treated as frequencies, which is worth noting. According to Flage & Røed (2012), when establishing likelihood categories, a decision must be made regarding the choice of likelihood unit. Clearly, this has not been done in IRAM<sub>2</sub>.

#### 4.3.2 Risk output

IRAM<sub>2</sub> attempts to unify information risk assessments with operational risk assessments and is apparently successful in its attempt to transform information risks. However, when examining the resulting risk output from the methodology, it does in fact not translate well into an overall ERM risk picture. The risk scoring system outputs a two-dimensional index where the likelihood dimension is based on a combination of qualitative criteria for each relevant risk driver (history, motivation, capability and commitment for adversarial threats), and the residual impact is a function of threat strength and control strength. To illustrate the issue with this output, the likelihood of initiation dimension will be considered.

Assume that the business impact categories covering monetary losses are the same categories used in other departments, i.e. the consequence scale used for determining financial risks is the same scale as used for determining consequences of information risks. Furthermore, assume that a risk practitioner wants to describe the total risk picture for the organisation in a risk matrix, covering all the different departmental risks. The practitioner is now faced with a problem with regards to inputting the information risk outputs from IRAM<sub>2</sub> into the overall ERM risk matrix.



**Figure 6 - InfoSec risk output and enterprise risk output**

Illustrated in Figure 6, it is not clear what a “high” likelihood on the y-axis in the information risk matrix would correspond to in the overall ERM risk matrix.

Risk matrices have some clear strengths, as discussed in [Section 2.3](#). They are simple to use and can communicate risk results in an intuitive fashion. However, one must be careful when using categories that introduce quantities that are hard to explain (see (Aven, 2015, p. 145), such as 0-3 used in IRAM<sub>2</sub>. There is a prioritised residual risk profile accompanying the risk matrix in IRAM<sub>2</sub>. This list gives an overview over:

- threat
- threat event
- residual likelihood
- residual impact rating
- residual risk rating

Presenting the risk output this way clearly states what the magnitude of the likelihood and the impact is. This provides more information regarding a risk, compared to just listing the residual risk rating without the corresponding dimensions that output the risk.

#### 4.3.3 Background knowledge and uncertainty

The methodology does not highlight the importance of quality of background knowledge and the hidden uncertainties, nor does it incorporate the strength of knowledge in the risk presentation. To properly describe risk there is a need to see beyond the likelihoods/probabilities that only express the degree of belief regarding the occurrence of an

event given some background knowledge. The example in (Aven, 2015, pp. 24-25) illustrates the issue:

For a coin toss with a normal coin you assign the probability of heads to be 0.5. This probability judgement can be based on that the symmetry of the coin means both sides are equally likely, and that your experience with this specific coin supports getting head about half the time you throw it. The background knowledge for this probability assignment can be considered strong. Next situation, you are to assign the probability of a new and unknown (to you) coin. This coin could be a fake, designed to land more often on, e.g. heads than tails. You do not have this information and will probably assign a probability of 0.5 for heads, but now the background knowledge is weak. Both situations are assigned the same probability, but for the first situation the background knowledge is strong, while for the second situation the background knowledge is weak.

This shows the importance of considering the background knowledge when assessing the strength of an assigned likelihood/probability. Applied to information security, knowing the background knowledge can be crucial in situations such as when there is a need to prioritise which threats to implement measures against. After having derived the residual risk rating in the last step IRAM<sub>2</sub>, for each information risk and having created a prioritised residual risk profile, there is no information regarding the strength of the background knowledge for the risks that have been calculated.

#### 4.4 Other

##### **Business impact ratings**

Business impact rating definitions in the financial category suffer overlap (see Table B.2: Example of a business impact reference table in IRAM<sub>2</sub> (2017, p. 22)). The financial numbers defining each category “negligible”, “low”, “moderate” and “high”, are respectively “<5k”, “<50k”, “<150k” and “>150k”. Mathematically, the “moderate” level covers the lower categories, making them redundant. The same problem is present for the percentage division for each category.

##### **Threat attribute definitions**

It is not clear how to interpret some of the threat profiling reference tables (TPRT) in Appendix D (Information Security Forum, 2017, pp. 65-69). Regarding the adversarial profiling of threat attributes capability and motivation, the table does not explicitly state if one, some, or all points for each rating needs to be fulfilled to classify as a specific rating. This is a central part of determining the likelihood of success and should be clearly defined.

The rating for the threat attribute “commitment” description suggests that it is needed in-depth knowledge regarding the resources of a potential threat:

“...threat expends at least 50% of its effort and/or computing/network resources initiating threat events against the organisation’s information systems being assessed, for a significant period of time (e.g. from weeks to months).”

It can be questioned how realistic it is to possess such accurate information regarding the threat actors.

#### 4.5 Conclusion

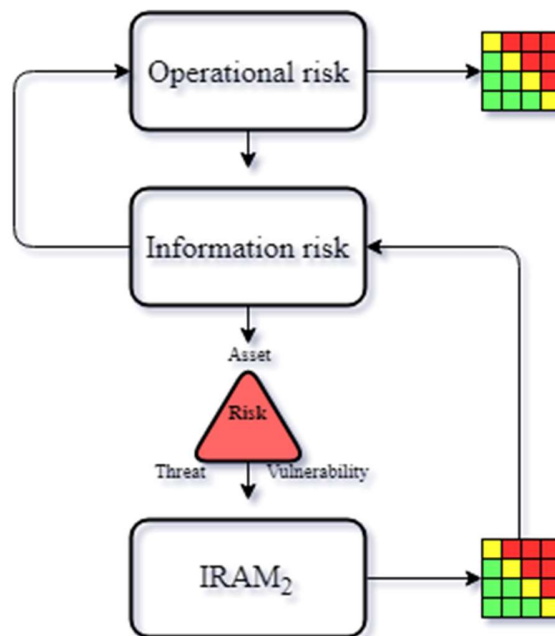
IRAM<sub>2</sub> is a practical methodology that complies with many of the guidelines in ISO. There are several holistically good aspects of the methodology in terms of the assessment process and having good principles. However, this work has also exposed weaknesses in the methodology, such as in the calculation methods used. Below is a summary of the advantages and limitations found throughout this work.

<b>Advantages</b>	<b>Limitations</b>
<ul style="list-style-type: none"> <li>• Concepts tailored towards InfoSec are well-defined and precise</li> <li>• Complies with most of ISO guidelines on principles for effective risk management</li> <li>• Process structure is closely related to the tried and tested ISO process, and is easy to follow</li> <li>• Methodology covers the whole lifecycle of risk management</li> </ul>	<ul style="list-style-type: none"> <li>• Generic, basic concepts related to the risk field are not good</li> <li>• Risk calculation methods seem arbitrary and unreliable</li> <li>• Risk scoring system is flawed</li> <li>• Risk matrix output does not translate well into how risk is considered in most enterprise risk management methods</li> <li>• Does not highlight the importance of background knowledge and uncertainty</li> <li>• Business impact ratings need correction</li> <li>• Threat attribute definitions are unclear</li> </ul>



## 5 Improving IRAM<sub>2</sub> and information security risk assessments in general

Figure 5 illustrates the connection between operational risk, information risk and IRAM<sub>2</sub>. As explained in [Section 2.4](#), information risk is a sub-domain of operational risk. Information risks are commonly assessed using the three-factor approach. In accordance with this perspective, IRAM<sub>2</sub> uses the three-factor approach as input and outputs residual risk ratings in a risk matrix with the commonly used dimensions of consequence (impact) on the x-axis and likelihood on the y-axis. Further use of this risk assessment would be to appropriately inform the management at the corporate level about the risk picture within operational risk, as part of an overall risk picture. Ideally, these information risks are then input into the overall operational risk picture, conveniently being on the same form.



**Figure 7 – Connection between operational risk and IRAM<sub>2</sub>**

From examining the findings, IRAM<sub>2</sub> manages to unify information security with operational risk to some degree. As explained with reference to Figure 7, with the three-factor risk assessment model as input, IRAM<sub>2</sub> outputs a risk matrix that can be further connected to how risk is assessed in operational risk assessments. However, there is room for improvements in several aspects alluded to in [Section 4](#). Some of these issues are well-known within the scientific field of risk and are not specific only for IRAM<sub>2</sub>. The main contribution from this report will be to look at a select few issues that, by improving them, could help ensure a more balanced reporting of information security risks to the top management and the board. These main contributions will be to;

- Add a set of criteria for assessing the strength of knowledge related to the probabilities.
- Improve risk scoring system
- Clarify subjective probabilities/qualitative judgements.

In addition, some minor quick fixes to IRAM<sub>2</sub> will also be suggested.

## 5.1 Criteria for strength of knowledge

The assigned probabilities for likelihood of initiation, threat strength and control strength are based on some knowledge (assumptions, data/information, expert knowledge, etc.), but this is not reflected in the results. As argued in [Section 2.2](#), to describe risk there is a need to see beyond the likelihoods/probabilities. They only express the degree of belief regarding the occurrence of an event, given some background knowledge, and the strength of this knowledge may vary. Knowing the strength levels that lie behind the residual risks can be crucial information when deciding how to prioritise risk reducing measures. Think of two situations (Askeland, Flage, & Aven, 2017, p. 2): one where the practitioner has strong background knowledge supporting the probability and consequence assignments of a threat event. Call this risk for R<sub>1</sub> and say that it was rated “moderate”. And another where, the practitioner has weak background knowledge supporting the probability and consequence assignments of a second threat event. Call this risk for R<sub>2</sub> and say it was rated “moderate”, i.e. same rating as the first risk. These two situations are different with respect to risk. Since R<sub>2</sub> is based on weak background knowledge, maybe it is in reality a “high” risk. But, the probabilities themselves do not reflect the uncertainty tied to the assumptions made regarding the risk.

This limitation of probability can be solved by adding judgements in regards to the strength of knowledge (SoK) about the probability assignments (Askeland et al., 2017, p. 2). To properly characterise risk, the suggestion is to better reflect the knowledge aspect of risk by using a set of criteria to assess the strength of knowledge.

Building on the risk concept and characterisation introduced in [Section 2](#), the uncertainty measure Q will cover subjective (knowledge-based/judgemental) probabilities P, or related interval (imprecision) probabilities, and judgement of the strength of the knowledge K (SoK) supporting these probabilities (Aven, 2017, p. 3). Thus,  $Q = (P, \text{SoK})$ .

To assess the strength of knowledge, a scoring system similar to what is recommended by Askeland, Flage & Aven (2017), can be used. Following are proposed criteria for the classification for strength of knowledge (SoK), adjusted to fit IRAM<sub>2</sub>. The SoK categories range from strong, moderate, to weak. It is proposed to assess the SoK for each threat.

**Strong** (All conditions are fulfilled, whenever relevant)

1. The threat profile is well understood
  - a. Threat origin is known
  - b. Relevant threat attributes are well understood
2. Associated threat events that a threat could initiate are well understood

- a. Threat event catalogue used for scoping has required accuracy
- b. Threat is identified and mapped to each in-scope threat event
- c. Information assets impacted by each threat event is identified and mapped
- d. Highest realistic and worst-case impact assessments for confidentiality, integrity and availability for each information asset is considered to be accurate
3. Much reliable data are available
4. There is broad agreement among experts
5. The knowledge K has not been scrutinised

**Moderate**

Conditions between strong and weak

**Weak** (At least one of the conditions are fulfilled)

1. The threat profile is not considered well understood
  - a. Threat origin is unknown
  - b. Relevant threat attributes are considered poorly understood
2. Associated threat events that a threat could initiate are not well understood
  - a. Threat event catalogue is incomplete/not up to date/inaccurate
  - b. Threat and in-scope threat event relationships are unclear
  - c. Information assets impacted by each threat event identification and mapping is incomplete/inaccurate
  - d. Highest realistic and worst-case impact assessments for confidentiality, integrity and availability for each information asset is considered to be inaccurate
3. No reliable data are available
4. There is considerable disagreement among experts
5. The knowledge K has been thoroughly scrutinised

Using the prioritised residual risk profile table from IRAM<sub>2</sub> (2017, p. 51) as basis, the SoK criteria could be reported as shown in Table 19.

<b>Risk ref.</b>	<b>Threat</b>	<b>Threat event</b>	<b>Residual likelihood</b>	<b>Residual impact rating</b>	<b>Residual risk rating</b>	<b>SoK</b>
<b>1</b>	Individual hacker	Unauthorised access to legitimate authentication credentials	Moderate	High	High	Strong

**Table 19 - Residual risk profile with SoK judgement**

The framework should cover phenomenological understanding/models, data, expert statements and assumptions and also the extent to which the knowledge base has been scrutinised (Askeland et al., 2017, p. 6). This is just a first attempt at constructing useful criteria for the information security field.

The likelihood dimension within information security is inherently challenging to determine. Since the likelihood is mostly based on qualitative judgements, at least within IRAM<sub>2</sub>, it is important that the strength of knowledge is assessed and expressed. This will ensure that no more weight is placed on the probability numbers than can be justified (Askeland et al., 2017, p. 7).

## 5.2 Risk scoring system

It is recommended to make changes to the current risk scoring tables used in IRAM<sub>2</sub> and how to derive the ratings. Table 20 shows the IRAM<sub>2</sub> risk factor scoring table that is used for both likelihood of initiation and threat strength.

<b>LoI/TS for adversarial threats</b>	
<b>6</b>	High
<b>5</b>	High
<b>4</b>	Moderate
<b>3</b>	Moderate
<b>2</b>	Low
<b>1</b>	Low
<b>0</b>	Negligible

**Table 20 – IRAM<sub>2</sub> risk factor scoring table**

As explained in [Section 3.4.3](#), the history attribute rating is summed with a motivation attribute rating to get the total score for the likelihood of initiation. This is not a reliable approach (see [Section 4.3.1](#)) and will be illustrated with two examples for the derivation of likelihood of initiation. First example uses the old risk scoring system and the second example will demonstrate the use of the new risk scoring system.

## Old system

The practitioner is to determine the correct rating for the history attribute for threat X. By reading the Threat Profiling Reference Tables (Information Security Forum, 2017, p. 66), the practitioner decides that the highest rating, 3, is the correct one:

“The threat is known to have initiated multiple and varied threat events (e.g. reconnaissance, physical attack, gaining unauthorised access and theft of information) relating to the environment over a predefined period of time (e.g. the previous 12 months)”

Next, the practitioner is to set the rating for the threat attribute “motivation”. To the knowledge of the practitioner, this threat is not expected to have any motivation for targeting the practitioner’s organisation. The rating that aligns with this characterisation:

“The threat is not expected to initiate a threat event against the environment”

This corresponds to a “negligible” rating, zero. Total risk factor score for this threat is, by summing the two scores and looking at Table 21, results in a “moderate” rating, 3.

## New system

Instead of an arbitrary summing system, it is recommended to treat the threat attribute assessment differently. The suggestion is to assign a LoI probability, based on what the practitioner knows regarding the relevant threat attributes. In this case, the practitioner makes use of the same Threat Profiling Reference Tables for history and motivation. Based on this knowledge, he sets a total probability for threat X, using Table 21.

<b>LoI for adversarial threats</b>	
<b>65-100%</b>	High
<b>40-65%</b>	Moderate-high
<b>20-40%</b>	Low-moderate
<b>0-20%</b>	Low

**Table 21 - Proposed risk scoring table**

The practitioner has information that the threat is known to have initiated multiple and varied threat events the last 12 months. As far as the practitioner knows, this threat should not be motivated to initiate threat events. There is no reason to believe that this threat is expected to initiate a threat against the environment. However, this is the case, even though the practitioner cannot find a justification for it. Recently, multiple and varied threat events have occurred, and

the practitioner judges this threat as very relevant, despite not understanding the threat's motivation. The result of this assessment:

$$P(\text{threat } X | \text{history, motivation}) = \text{High}$$

This approach makes use of the information in IRAM<sub>2</sub> found in the Threat Profiling Reference Tables. Furthermore, it does not restrict the threat level for a certain threat, based on e.g. having no prior knowledge about history. The old method would limit the potential threat to a “moderate” level in that case. This new system appreciates that a threat could still be rated e.g. “high” despite lacking information on one of the threat attributes.

Table 21 can also be used to determine Likelihood of success (LoS). LoS consists of the two components Threat Strength (TS) and Control Strength (CS). TS can then be considered as inherent LoS (that is LoI x TS equals inherent likelihood), while CS and TS together give residual LoS. CS should in this context be seen as a percentage reduction in the threat strength.

### 5.3 Other improvements

Following there will be presented other suggestions for improvements.

#### **Clarifying subjective probabilities**

It is crucial that the meaning of the probabilities is communicated when reporting risk assessment results. Subjective probability is characterised by an individual's personal degree of belief whether a specific outcome is likely to occur (Oredsson, 2017). This is important to convey, because people will interpret prior knowledge about an event differently. If the risk practitioner assigns a probability of, e.g. 0.9 for a specific threat event within the next 12 months, he needs a way to explain what this statement means. To ensure proper communication of subjective probabilities, it is advised to use an uncertainty standard proposed by Dennis Lindley, which Aven (2013, p. 2) is an advocate of:

“If a person assigns a probability of 0.1 (say) for an event A, he or she compares his/her uncertainty (degree of belief) of A occurring with drawing a specific ball from an urn containing 10 balls. The uncertainty (degree of belief) is the same.”

With this standard, common probability rules can be established. Presenting subjective probability in this way makes it easy to communicate as it separates between uncertainty and utility (Oredsson, 2017, p. 8). This interpretation can be used in any type of setting and does not require any formal education in statistics to understand the meaning of it.

#### **Business impact assessment intervals**

Business impact rating definitions in the financial category that suffer overlap (see [Section 4.4](#)): This problem is easily solved by defining unambiguous intervals for each impact rating. In this case, the impact ratings from negligible to high should be defined as: [0, 5k), [5k, 50k), [50k, 150k), [150k, inf). Square brackets indicate that the corresponding starting point is included in the interval. Parentheses indicate that the end point is not included.

## 6 Discussion

### 6.1 Overall considerations

IRAM<sub>2</sub> is a comprehensive methodology that covers not only the risk assessment process, but also gives the practitioner in-depth knowledge of risk from ISF's perspective. Risk is a fundamental concept in the context of information risk. Therefore, it is important that the practitioner receives some education on risk conceptualisation. However, some of the generic concepts related to risk have been criticised in this report, such as likelihood and risk. IRAM<sub>2</sub> emphasises the importance of engaging the right stakeholders. The practitioners of IRAM<sub>2</sub> is presented with a complete 'package' in this sense, that covers the whole lifecycle of risk management. It has some real advantages, such as a process structure that is very similar to ISO 31000 (2018), which is trusted in many industries.

Today, information security risk assessments are commonly based on threats, vulnerabilities and asset evaluations. IRAM<sub>2</sub> uses this approach and outputs a risk matrix. Limitations have been identified in IRAM<sub>2</sub> in connection with how the risk assessments are carried out. One of the critical limitations of this methodology is in relation to the derivation of information risks.

The information risk equation used in IRAM<sub>2</sub> builds on the traditional equation where risk is the product of likelihood and impact. But, the two components are not multiplied at any stage. The equation is decomposed into several different levels, best illustrated by Figure 4 in [Section 3.4](#). Likelihood of initiation (LoI) and threat strength (TS) are derived by summing certain threat attributes to reach a risk score. The limitations of the derivation of LoI has been discussed, which is two-fold; using the threat attribute history as a factor that drives the rating, and the summing of the threat attributes. The latter is the same issue found with the derivation of TS. Furthermore, the control strength (CS), which has not been discussed, is derived by applying a formula (see [Section 3.4.4](#)). This formula accounts for the relevance of the control and the level of implementation of the control. It seems logical that the control strength is dependent on these two factors. However, further work would be needed to verify if the approach for determining control strength is reliable.

The methodology uses matrices for two different means, namely as a classification matrix and a traditional matrix with impact on the x-axis and likelihood on the y-axis. The likelihood of success is found after determining the threat strength and control strength. This is done by using the classification matrix to read off the correct rating for Likelihood of success (LoS) (see Table 16 in [Section 3.4.5](#)). The residual likelihood is then found by using another classification matrix to read off the rating that intersects LoI and LoS (see Table 17 in [Section 3.4.5](#)). Finally, after having determined the residual impact, the residual risk can be determined. This shows that there are many steps that need to be taken to eventually reach a risk score, and one can assume that the process quickly gets complex as the practitioner attempts to map all relevant risks that an organisation is exposed to.

Having finished this process, the practitioner can present the information risks in a risk matrix. Alternatively, the practitioner can choose to present the prioritised residual risk profile in a table as suggested in IRAM<sub>2</sub>. The output from IRAM<sub>2</sub> does not reconcile with risk output from risk domains on higher levels, such as operational risk. The risk output from IRAM<sub>2</sub> is not in absolute terms and there is no clear way of how to convert them. With the current approach, there is no way of combining information risk assessments with enterprise risk management reporting, as shown in [Section 4.3.1](#). Enterprise risk management models are designed to compare risk levels for all types of domains. This means that the risk dimensions, e.g. (C,P), must be on the same form. This poses a challenge for the risk practitioner that needs to disseminate the results in combination with other risk domains to the top management.

## 6.2 Bridging the gap

Improvements are proposed regarding strength of knowledge criteria, improving risk scoring system and clarifying subjective probabilities. Incorporating these improvements will aid in bridging the gap between information security assessments and enterprise risk management reporting. But, to reach the full potential of the provided improvements, more work is needed.

### Strength of knowledge

The strength of knowledge criteria can be an important aid in expressing the assessor's knowledge regarding the subjective judgements. But the suggestion in [Section 5.1](#) can be further enhanced by splitting the strength of knowledge criteria for residual likelihood and the residual impact.

<b>Risk ref.</b>	<b>Threat</b>	<b>Threat event</b>	<b>Residual likelihood</b>	<b>SoK</b>	<b>Residual impact rating</b>	<b>SoK</b>	<b>Residual risk rating</b>
<b>1</b>	Individual hacker	Exploit vulnerable authorisation mechanisms	Moderate	Weak	High	Strong	High

**Table 22 - Residual risk profile with SoK judgements for likelihood and impact**

This results in more accurate assessments of the strength of knowledge, as the criteria is tailored specifically to each of the two dimensions. The practitioner can then communicate more accurately what the results are built on. Table 22 is an example of what this should look like, by using the prioritised residual risk profile table from IRAM<sub>2</sub> (2017, p. 51) as basis.



## **Risk scoring system**

By changing the risk scoring system as proposed in [Section 5.2](#), IRAM<sub>2</sub> can output probability estimates that correspond with other risk management models. By also making changes to the consequence dimension, the information risk assessments from IRAM<sub>2</sub> can be represented in an overall risk management model. If the probabilities were derived as suggested in [Section 5.2](#), they would be assigned as probability intervals, which correspond to more commonly used dimensions. But, these probabilities make more sense if they are defined within a certain time frame. It is suggested to convert them into a frequency, the expected rate of occurrence in a standard unit of time, which is usually a year.

The idea of using the Threat Profiling Reference Tables provided in IRAM<sub>2</sub> as basis for setting an overall rating needs more work. The approach should be structured and easy to follow for the risk practitioner. This is important because it will help in producing consistent and reliable assessments. After making the changes suggested regarding the scoring system, a natural segue would be to assess if the list of threat attributes characterising adversarial threats is complete. As stated in (Wangen, Shalaginov, & Hallstensen, 2016), the threat assessment process relies on the quality of threat intelligence and understanding of the adversary. Maybe other threat attributes should be considered, such as; motive, primary intent, preferred targets or personal risk tolerance (Freund & Jones, 2014).

It cannot be claimed that the complete answer to bridging the gap between information security and enterprise risk management has been found. However, the gap will be smaller if the proposed improvements are implemented. IRAM<sub>2</sub> is a methodology with many holistically good aspects in terms of the assessment process and having good principles. With some further work on the suggested improvements, IRAM<sub>2</sub> could be a viable option as a risk assessment framework that fits within an overall enterprise risk management model.

## **6.3 Further work**

### **Other aspects of IRAM<sub>2</sub> not covered**

As mentioned in [Section 6.1](#), the control strength formula has not been evaluated in this report. The formula consists of two components; control relevance and control implementation. It would be necessary to evaluate this formula and the related scoring table and find a good way to implement the new scoring system. IRAM<sub>2</sub> provides Control relevance tables (CRT) which aid the practitioner in understanding a control's ability to deliver protection. A control library is also available. These are comprehensive tables. It would be of interest to investigate how often these lists should be updated to stay relevant in the ever-evolving cyber threat landscape. This also holds true for what types of threat events one can expect.

The procedure for setting the residual business impact rating would also be of importance for further work. In IRAM<sub>2</sub>, the practitioner first decides on the inherent business impact for each risk. Further, it is assessed if this rating is appropriate to apply, or if there is a need for adjusting

this rating. This is done by using the Likelihood of success matrix, which is connected to Control strength and Threat strength.

The focus has been on adversarial threats throughout this work. Accidental and environmental threats should also be investigated to look for potential improvements in how they are assessed. They are built on the same reasoning as adversarial threats, and most likely there are only small adjustments necessary to make the proposed improvements applicable to the other threat categories.

The use of subjective probabilities within the security domain has a well-known problem ((Aven, 2014, p. 10), (Brown & Jr, 2011)) which should be just as relevant for the information security domain and is worth mentioning. Specifying the subjective probabilities is connected directly to risk management responses. The issue that is pointed to is the fact that the behaviour of human threat actors may vary depending on what they know regarding what we, as the analysts, know. For example, the practitioner might assign a high likelihood score for a specific threat event, resulting in that this type of threat is prioritised, and protective measures are implemented. But because of this fact, the potential threat actor might conclude (after gathering information, doing reconnaissance) that the probability of success for this attack has now been reduced to the point that it is not worth engaging an attack. The result is that the risk practitioner's initial assigning of a high likelihood can no longer be considered high, but the practitioner has no way of knowing this. Cox (2008, p. 11) argues that threat estimates might be self-defeating if the attackers use intelligence about the defender's own threat estimates to help decide where and when to attack. The context is terrorist attacks, but the same principles could be applicable to the behaviour of threat actors within information security.

### **Bayesian networks**

A Bayesian network (BN) is a probabilistic model based on directed acyclic graphs. Directed acyclic graphs are finite directed graphs with no directed cycles (Pearl, 2011). The BN visualises the causal interactions for certain problem domains and can be useful for modelling uncertainty in security analysis (Xie, Li, Ou, Liu, & Levy, 2010). One suggestion for further work is to convert IRAM<sub>2</sub>'s information risk equation into a Bayesian network.

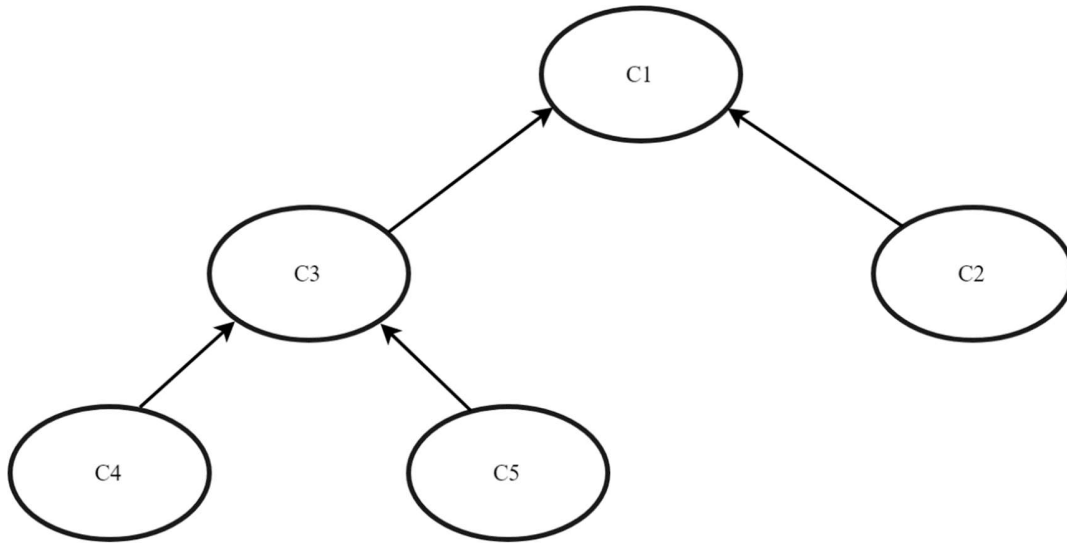


Figure 8 - BN for IRAM<sub>2</sub>

A starting point for this work is to rearrange the information risk equation as proposed in Figure 8. C1 is the residual risk, C2 residual impact, C3 residual likelihood, C4 likelihood of initiation and C5 is likelihood of success. The specific expression for the compound distribution described by this network:

$$P(c_1, \dots, c_5) = \prod_{i=1}^5 P(c_i | pa(c_i)) = P(c_1, |c_2, c_3) \times P(c_2) \times P(c_3 | c_4, c_5) \times P(c_4) \times P(c_5)$$

The models are easy to update with new information and provides a systematic approach for combining knowledge (Oredsson, 2017, p. 13). The evidence suggests that a BN can be a good approach for assessing information risks, as the method can model situations where little data is available but there is expert knowledge regarding a threat. The BN can handle uncertainty efficiently, although it depends on having informative priors which will lead to higher accuracy in the posterior inferences (S. D. Guikema, 2007). Turning IRAM<sub>2</sub> into a Bayesian network could be an interesting approach and in combination with the advantages of IRAM<sub>2</sub>, such as having good framework principles and a structured process, could potentially turn it into the preferred risk assessment methodology within the information security field.

## 7 Conclusion

Current practice for information security risk assessment, as represented by IRAM<sub>2</sub>, has been evaluated in this report. At present time, information security risk assessment methods are not well integrated into operational risk/enterprise risk management models. Several weaknesses have been found in IRAM<sub>2</sub>. The most significant relate to calculation methods, a flawed risk scoring system, and a risk matrix output that does not translate well into how risk is considered in most risk management models. The methodology does not highlight the importance of background knowledge and hidden uncertainties. [Section 4.3.2](#) shows that IRAM<sub>2</sub> does not unify information security risk assessments with risk assessments in other risk domains that exist within an enterprise. The suggestions that are provided will improve IRAM<sub>2</sub>, and the information security risk field in general. These suggestions include adding a set of criteria for strength of knowledge related to the qualitative judgements of the likelihood of a threat, and change the risk scoring system so that the risk output can be presented in risk matrices at the corporate level. A suggestion is presented on how to advance the reporting of information risks to the decision makers. To clarify subjective probabilities, it is recommended to use an uncertainty standard. The complete answer to bridging the gap between information security and enterprise risk management has not been found, however, several improvements have been identified that will make the gap smaller.

## 8 References

- Andress, J. (2014). *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*: Syngress.
- Askeland, T., Flage, R., & Aven, T. (2017). Moving beyond probabilities—strength of knowledge characterisations applied to security. *Reliability Engineering & System Safety*, *159*, 196-205.
- Aven, T. (2010). On how to define, understand and describe risk. *Reliability Engineering & System Safety*, *95*(6), 623-631.
- Aven, T. (2011a). *Misconceptions of risk*: John Wiley & Sons.
- Aven, T. (2011b). On how to conceptualise and describe risk. *Reliability: Theory & Applications*, *6*(1 (20)).
- Aven, T. (2011c). On the new ISO guide on risk management terminology. *Reliability Engineering & System Safety*, *96*(7), 719-726.  
doi:<https://doi.org/10.1016/j.ress.2010.12.020>
- Aven, T. (2013). On the meaning of a black swan in a risk context. *Safety Science*, *57*, 44-51.  
doi:<https://doi.org/10.1016/j.ssci.2013.01.016>
- Aven, T. (2014). *Risk, surprises and black swans : fundamental ideas and concepts in risk assessment and risk management*. Abingdon, Oxon ; New York, NY: Routledge, Taylor & Francis Group.
- Aven, T. (2015). *Risk analysis*. Chichester, West Sussex, United Kingdom: Wiley.
- Aven, T. (2017). Improving risk characterisations in practical situations by highlighting knowledge aspects, with applications to risk matrices. *Reliability Engineering & System Safety*, *167*, 42-48. doi:<https://doi.org/10.1016/j.ress.2017.05.006>
- Aven, T., & Reniers, G. (2013). How to define and interpret a probability in a risk and safety setting. *Safety Science*, *51*(1), 223-231. doi:<https://doi.org/10.1016/j.ssci.2012.06.005>
- Brown, G. G., & Jr, L. A. C. (2011). How Probabilistic Risk Assessment Can Mislead Terrorism Risk Analysts. *Risk Analysis*, *31*(2), 196-204. doi:10.1111/j.1539-6924.2010.01492.x
- Committee, C. A. S. E. R. M. (2003). Overview of enterprise risk management. *Fairfax, VA: Casualty Actuarial Society*.

- Cox Jr, L. A. T. (2008). Some limitations of “Risk= Threat× Vulnerability× Consequence” for risk analysis of terrorist attacks. *Risk Analysis*, 28(6), 1749-1761.
- Cox, L. A. (2008). What's wrong with risk matrices? *Risk Analysis*, 28(2), 497-512. doi:10.1111/j.1539-6924.2008.01030.x
- D’Arcy, S. P., & Brogan, J. C. (2001). Enterprise risk management. *Journal of Risk Management of Korea*, 12(1), 207-228.
- Flage, R., & Røed, W. (2012). *A reflection on some practices in the use of risk matrices*. Paper presented at the 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012, PSAM11 ESREL 2012.
- Freund, J., & Jones, J. (2014). *Measuring and managing information risk: a FAIR approach*: Butterworth-Heinemann.
- Guikema, S. (2012). Modeling intelligent adversaries for terrorism risk assessment: Some necessary conditions for adversary models. *Risk Analysis*, 32(7), 1117-1121.
- Guikema, S. D. (2007). Formulating informative, data-based priors for failure probability estimation in reliability analysis. *Reliability Engineering & System Safety*, 92(4), 490-502.
- Information Security Forum. (2017). Information Risk Assessment Methodology 2 (IRAM<sub>2</sub>). In *The next generation of assessing information risk*: Information Security Forum Limited.
- International Organization for Standardization. (2011). NS-ISO 27005:2011. In *Information technology - Security techniques - Information security risk management* (pp. 76).
- International Organization for Standardization. (2013). NS-ISO/IEC 27001:2013. In *Information technology - Security techniques - Information security management systems - Requirements* (pp. 23). Norway: Standard Norge.
- International Organization for Standardization. (2017). NS-ISO 27000:2017. In *Information technology - Security techniques - Information security management systems - Overview and vocabulary* (pp. 34). Norway: Standard Norge.
- International Organization for Standardization. (2018). NS-ISO 31000:2018. In *Risk management - Guidelines* (pp. 28). Norway: Standard Norge.
- Oredsson, M. (2017). *RIS610 Selected topics in risk management*. Retrieved from N/A
- Pearl, J. (2011). Bayesian networks.
- Refsdal, A., Solhaug, B., & Stølen, K. (2015). *Cyber-risk management*. Cham; Heidelberg [u.a.]: Springer.

- SRA. (2015). SRA Glossary. In *Society for Risk Analysis Glossary*.  
[http://www.sra.org/sites/default/files/pdf/SRA\\_glossary\\_20150622.pdf](http://www.sra.org/sites/default/files/pdf/SRA_glossary_20150622.pdf).
- Supervision, B. C. o. B. (2011). Principles for the Sound Management of Operational Risk. In.  
[www.bis.org](http://www.bis.org): Bank for International Settlements.
- The Committee of Sponsoring Organizations of the Treadway Commission. (2018). *Enterprise Risk Management - Integrated Framework*. Retrieved from  
<https://www.coso.org/Pages/erm-integratedframework.aspx>
- von Solms, R. (1998). Information security management (3): the Code of Practice for Information Security Management (BS 7799). *Information Management & Computer Security*, 6(5), 224-225. doi:10.1108/09685229810240158
- Wangen, G., Shalaginov, A., & Hallstensen, C. (2016). *Cyber Security Risk Assessment of a DDoS Attack*. Paper presented at the International Conference on Information Security.
- Xie, P., Li, J. H., Ou, X., Liu, P., & Levy, R. (2010). *Using Bayesian networks for cyber security analysis*. Paper presented at the Dependable Systems and Networks (DSN), 2010 IEEE/IFIP international conference on.