A Risk Assessment of the Insider Threat in Commercial Aviation

- The IRGC Risk Governance Framework Approach

Student: Anna Dietzel (s1889338)
Course of Study: MsC Crisis and Security Management
Supervisor: Ludo Block
Second Reader: Tim Dekkers
Submitted: June 10th 2018
Word count: 18853 (continuous text)
Acknowledgements

A special thank you,

to my supervisor, Ludo Block, for guiding me through this process called thesis and helping me write a short yet informative story;
to the airline for accepting my research request and taking the time to talk to me and introduce me to their work;
and to my family, friends and Andi for supporting me throughout my studies.
This Thesis seeks to research the applicability of the risk governance framework by the International Risk Governance Council to the risk of the insider threat in aviation. To exert the framework information on the phenomenon *insider threat* is needed. As research is still fragmentary on this, particularly on airlines' management of the risk, a single case study is conducted to close the information gap. The case is a commercial airline. In order not to infringe the airline's security efforts on this matter, it is referred to in an anonymised manner throughout the thesis. All data collected for the case study is documented in the unpublished confidential Appendix.
Table of Content

1. Introduction ........................................................................................................................................... 1
   1.1 A new Threat in Aviation ................................................................................................................. 1
   1.2 Societal and Academic Relevance .................................................................................................. 1
   1.3 Research and Sub-Research Questions ............................................................................................ 3
   1.4 Research Outline ............................................................................................................................ 4

2. Literature Review .................................................................................................................................... 5
   2.1 'Risk' in Security Studies .................................................................................................................. 5
       2.1.1 Risk ........................................................................................................................................... 5
       2.1.2 Security Studies and Risk Studies .............................................................................................. 6
   2.2 Aviation Security and the 'Insider Threat' in Literature .................................................................... 7
       2.2.1 Aviation Security ....................................................................................................................... 7
       2.2.2 Aviation's Insider Threat ........................................................................................................... 8
       2.2.3 Aviation's Insider Threat in Academic Literature ...................................................................... 10

3. Theoretical Framework: The IRGC Risk Governance Framework ....................................................... 14

4. Methodology ........................................................................................................................................... 17
   4.1 Research Design ............................................................................................................................... 17
   4.2 Data Collection .................................................................................................................................. 18
   4.3 Concepts and Operationalization ...................................................................................................... 20
   4.4 Pitfalls and Limitations .................................................................................................................... 22

5. Case Study: The Airline .......................................................................................................................... 24
   5.1 The Airline's Safety and Security Department .................................................................................. 24
   5.2 Understanding and Approach of Risks ............................................................................................. 25
       5.2.1 Definitions and Understandings ................................................................................................. 25
       5.2.2 The Risk Management Guideline ............................................................................................... 25
   5.3 The Airline's Insider Threat .............................................................................................................. 29
       5.3.1 Definition .................................................................................................................................... 29
       5.3.2 Evaluation of Insider Threat based on Risk Management Guideline ......................................... 30
   5.4 Project Insider Threat ....................................................................................................................... 31
   5.5 Crew Members as Insider ................................................................................................................. 33

6. Hitherto Conclusions ............................................................................................................................. 35
   6.1 Answers to Sub Research Questions ............................................................................................... 35
   6.2 Reflection on the Case Study ........................................................................................................... 35

7. The IRGC Framework Applied ............................................................................................................. 38
   7.1 Pre-Assessment .................................................................................................................................. 38
   7.2 Appraisal .......................................................................................................................................... 40
   7.3 Characterisation and Evaluation ....................................................................................................... 42
   7.4 Management ...................................................................................................................................... 43
7.5 Communication .......................................................... 44
7.6 Analysis ........................................................................ 44
8. Conclusion ........................................................................ 48
Bibliography ........................................................................ 50
List of Figures

Figure 1: Five Phases and their Components of the IRGC's Framework ........................................ 15
Figure 2: Distribution Risk Classes ................................................................................................ 27
Figure 3: Event Risk Classes ............................................................................................................. 27
Figure 4: Qualitative Risk Classes .................................................................................................... 28
Figure 5: Insider Threat Matrix
1. Introduction

1.1 A new Threat in Aviation

For a long time, passengers of commercial airplanes were seen as the greatest threat to aviation's security. The attacks of 9/11 strengthened this notion and saw a drastic increase in security measures. Most notably are scanning equipment for passengers before boarding their flight. Simultaneously employees in the industry were not considered a security risk, on the contrary they were and are trusted and have “nearly unfettered access to critical aviation infrastructure, aircraft, and equipment” (Loffi & Wallace, Part 1, 2014, p. 289). News organisations have increasingly brought forward reports on the risk of aviation's security from employees shedding the light on a new form of risk in the industry: the insider threat (p. 289-290).

Aviation's insider threat is to date a topic that has been researched only little. Cases of insiders harming the industry in different forms is unfortunately not only a risk in theory as there are several reported incidents. An Air China captain deviated from the planned route in 1998 to land the Boeing 737 he was flying in Taiwan, because he was unsatisfied with his salary and company policies. In 2014 five ramp workers were arrested at Logan Airport in the United States for smuggling drug money worth $417,000. In yet another case a Denver Airport Shuttle Driver was arrested in 2009 after it was discovered he had received training from al Qaeda in using weapons and building explosives. While he planned to target the New York Subway, his workplace could have easily become a target. As there are many incidents where the industry's insider posed a security threat (Loffi & Wallace, Part 2, 2014, p. 307-309), a demand for research regarding the topic is evident.

The following research will assess the applicability of the International Risk Governance Council's (IRGC) (IRGC, 2005) risk governance framework to the appraisal of the risk 'insider threat to commercial aviation'. To develop a deeper understanding of the insider threat one airline's security department will be investigated in regard to their approach to this risk. Based on these findings and the knowledge gained through the literature review the framework will be applied. Afterwards it will be evaluated to what extent the IRGC's framework is applicable when assessing the insider threat to commercial aviation.

1.2 Societal and Academic Relevance

In 2015, the International Air Transportation Association (IATA), publicly voice the concern of the risk of insider threats (IATA, 2015, p. 1). The United States Agency Transportation Safety Agency (TSA) even sees the insider threat as one of the most important ones the industry is facing today (Siao, 2017). An insider for this purpose is defined as “a person who exploits, or has intention
to exploit, their role or knowledge for unauthorized purposes. They may be full or part-time permanent employees, individuals on attachment or secondment, contractors, consultants, agency staff or temporary staff” (IATA, 2015, p. 1). The term 'insider' encompasses not only a large group of people but also significantly different occupations within the industry that allow persons to access different areas within the airport and aircrafts and differing knowledge on security procedures. For the purpose of the following research the term insider will be confined to cabin and cockpit crew in commercial aviation. This group of 'insiders' are in a unique position regarding their possibility to 'harm' the industry. They do not only have knowledge over the aircrafts they fly, its electronics, passengers and security procedures but also have control over the aircraft when it is airborne.

Studying airlines' approach to the insider threat, learning about the phenomenon and its possibly needed counter measures has societal relevance. Firstly, it has the potential to affect people worldwide with 4.1 billion commercial aviation passengers in 2017 (ICAO, 2018). Secondly, there have been incidents when crew, in these cases cockpit crew, 'harmed' the industry. Most prominently did the Germanwings crash of flight 4U9525 on March 24, 2015 raise awareness for an insider threat to aviation (Marino-Hernandez, 2015, p. 1). The flight's co-pilot deliberately flew the airplane into the French Alps to crash, after locking the captain out of the cockpit. All 144 passengers and 6 crew members died in the incident (p. 23). Another incident demonstrating that an inside threat is real, is the case of Ethiopian Airlines Flight ET 702 on February 17, 2014. Similar to the Germanwings case did the co-pilot lock the captain out of the cockpit when he left it to go to the toilet. He hijacked the plane and deviated from the planed route to fly to Geneva, Switzerland, to seek asylum. In this case no casualties were accounted (Abeyratne, 2014). Thirdly, the number of previous incidents caused by insiders suggest that the insider threat will increase in the future (Krull, 2016, p. 30) making the insider threat also a future hazard.

The study also bares an academic relevance. The concept risk is still fairly novel to the academic world, as it only found prominence in the 1970s and 1980s. Today risk analysis and risk assessments are a quintessential part of many societal sectors (Aven, 2016), also in aviation (CIOACĂ, 2011). The polysemic concept 'risk' can be defined as an “uncertainty about and severity of the consequences (or outcomes) of an activity with respect to something that humans value” (Aven & Renn, 2009 as cited in Roodenrijs, Kraaij-Dirkzwager, van den Kerkhof, Runhaar, 2014, p.1163). The academic field of 'risk' research has the purpose to enlighten the world on topics related to risk and how they can be addressed (Aven, 2016). On the particular issue of 'insider threats' in commercial aviation little is written, especially from a qualitative risk assessment or risk management point of view. So far definitions and driving factors have been established (Wallace and Loffi, 2014, Part 1; Krull, 2016). Further have security weaknesses been outlined and according mitigating measures
proposed (Wallace and Loffi, 2016, Part 2; Black, 2010). The possibility of insiders being motivated by terrorism has also been discussed (Krull, 2016; BaMaung, McIlhatton, MacDonald & Beattie, 2016). How this risk of an insider is perceived by airlines has not been explored yet, nor has research on an airline's practical management of this risk been published. To date there is no academic risk assessment of the insider threat to commercial aviation conducted based on the IRGC's framework. By using the IRGC's framework the gap between academic research and the practical application may be marginalized and the framework will be tested in the aviation industry. The concept of risk merging into security studies is a recent development (Petersen, 2011, p. 694-695), research within this new field of security studies will thus be a small contribution to a growing body of knowledge.

1.3 Research and Sub-Research Questions

The aim of this research is to add to the literature of the insider threat to commercial aviation by taking a security-risk perspective. For this purpose, the central research question of this proposed explanatory study is:

“To what extent can the Risk Governance Framework developed by the International Risk Governance Council be applied in the assessment of the insider threat to commercial aviation?”

In order to answer this question one airline is chosen as the subject of analysis regarding their general risk assessment process and their perception of the insider threat. For this purpose, three sub questions will be answered:

Sub question 1: “How does the airline assess risk?”
Sub question 2: ”Does the airline distinguish different categories of risk in their risk management and if so what are these categories?”
Sub question 3: “Is the insider threat a recognized threat, if so how is it measured and which category is it attributed to?”
1.4 Research Outline

In the following chapter a literature review on 'risk' in security studies, a brief discussion on the term 'insider threat' and relevant theory for the proposed research will be presented. As the assessment of the risk will be based on the IRGC's risk governance framework this method will be explained in chapter 3. Subsequent hereto in chapter 4 the research's methodology is outlined. Chapter 5 is about the case study on one airline and chapter 6 reflects on these findings. The assessment of the insider threat through the framework is conducted in chapter 7, as well as the analysis of its applicability. A final conclusion on the study is given in Chapter 8.
2. Literature Review

2.1 'Risk' in Security Studies

Risk studies are originally set within sociology, natural sciences and economics, while security studies are part of International Relation. For the longest time these two fields did not touch upon one another (Petersen, 2011, p. 694-695). Below the modern concept of risk will be discussed and a brief overview of the evolution of security studies will be presented. Thereafter the merging of the two academic fields will be outlined.

2.1.1 Risk

The concept of risk has been defined differently throughout time and is today still viewed from different angles whereby its definitions stress different aspects. In modern times risk “designate[s] the possibility for change” and “is associated with abandoning old constraints and entering new and better futures” (Petersen, 2011, p. 697). Risk is used to justify political actions and decisions. This interlinkage between risk and progress was manifested in the 17th century with the emergence of statistics and thinking in probabilistic terms and later the rise of investment risk, insurance and banking becoming a “calculable, quantifiable, classifiable and individualized entity” (p. 697). In the 20th century theories evolved surrounding risk as a 'measurable uncertainty' and by the 1970s risk management was an established practice in many corporations. It aims to “estimate the probability and present the economic value of future events” (p. 697). The concept of risk has been broadened by scholars and refers to a wide range of situations involving uncertainty such as private companies, crime, citizens etc. (p. 696-697). This conception of risk builds on the understanding that it can be quantified and classified (Aradau et al., 2008, p. 148). It can thus be defined as a “family of ways of thinking and acting, involving calculations about probable futures in the present followed by interventions into the present in order to control that potential future” (Rose, 2001, as cited in Aradau et al., 2008, p. 149).

Risks “are assessed according to frequency, the vulnerability of the assets involved, and the probable impact” (Salter, 2008, p. 252). Scholars often use the equation “Risk = Threat x Vulnerability x Consequences” to define them (Stewart & Mueller, 2013, p. 617). 'Consequences' at times are also referred to as 'Criticality', both describing the “magnitude of negative effects” (Tamasi & Demichela, 2011, p. 893). As the IRGC's framework is used in this research, their understanding of risk will be used throughout. Risk is defined by them as “an uncertain consequence of an event or an activity with respect to something that humans value” (Kates et al., 1985 as cited in IRGC, 2006, p. 19). Hereby it refers to the combination of “the likelihood or chance of potential consequences and the severity of
consequences of human activities, natural events or a combination of both” (IRGC, 2006, p. 19). Regarding the variables of a risk assessment, the IRGC also sees consequences, vulnerability and threat as the central components. Threat is within the IRGC framework expressed as a 'hazard'. 'Vulnerability' is “the various degrees of the target to experience harm or damage as a result of the exposure” (p. 27). Generally, threats are “quantifiable, specific and about intentions and means-ends rationality” (Petersen, 2011, p. 703). Central to the concept risk is further its subjectiveness. People perceive risks differently, whereby aspects, such as culture, emotions and experience play an influential role (IRGC, 2006, p. 31-33). This aspect of risk will be further discussed in chapter 3.

2.1.2 Security Studies and Risk Studies

'Security studies' developed as a sub discipline of International Relations (IR) (Baldwin, 1997, p. 16). For this development the years between the first and second World War were of great importance, when military force was replaced by arbitration, international understanding, international law and an emphasis on democracy to promote security and peace. During this period academics interest for the field rose and led to the opening of research centres, International Affairs Graduate Schools and journals dedicated to the topic. In this early stage of 'security studies' security was considered as 'national security' (COT, 2007, p. 6-7). This realistic point of view of traditionalists regards “security in exclusively military and state-centred terms” (p. 17). In the Cold War era the invention of nuclear weapons and their destructiveness changed the view on 'security'. The issue was approached through either balance of power, containment and deterrence or bipolar world (p. 7-8). Neither policymakers, academics or theories foresaw the end of the cold war which led to a debate on the credibility and validity of the existing theories and a reshaping of the concept 'security' (p. 13). In the 1980s and 1990s the 'security debate' in the academic sphere of security studies appeared to have been settled. The debate on what would be considered a security issue generated a “division between traditionalists and wideners” (Petersen, 2011, p. 700).

The concept 'security' is until today a contested one (Williams, 2013, p. 1) with no universal definition of the term (COT, 2007, p. 5). Often it is referred to as “the alleviation of threats to cherished values” (Williams, 2013, p. 6), demonstrating that it “means different things to different people” (p. 1). 'Vulnerability' and 'risk' are central to the concept, terms that again are “inescapably subjective assessment[s]” (Barnett, 2001, p. 24).

The concept 'risk' has found a place within the broader field of security studies, in the course of the security studies widening debate. The attention that transnational threats, climate change and terrorism have received has led to the fields of risk and security growing closer. A common research
theme and catastrophic events, demonstrated the need for a “common research agenda” (Petersen, 2011, p. 694-695). At the end of the cold war international organizations and major states further referred to “their security environment in terms of risks rather than dangers” (Aradau, Lobo-Guerrero & van Munster, 2008, p. 147). Comparing threat-based and risk-based perspectives to security shows how differently the question of security is addressed. The latter “tend to emphasize systemic characteristics, such as populations at risk of disease or environmental hazard” (p. 148). They depend on modelling, data and speculations that are used to establish strategies to face a risk, a contingency, instead of eliminating it. The threat-based perspective depends on “intelligence in an attempt to eliminate danger” (p. 148). Risk studies aim to contribute to discussions about political and social life. The scope on security studies should thereby be broadened and blur the dividing lines between economics, sociology and political science (Petersen, 2011, p. 701). Petersen identifies three schools of thought regarding the approach of risk within security studies: Critical Risk Studies, Global Risk Management and Political Risk Studies. Each focuses on only a small selected part of the risk literature representing one specific interpretation of economic and sociological theories (p. 694-695).

As previously mentioned the literature found on 'insider threats' is relatively slim. Nevertheless, have authors managed to lay a base for further research into the issue. This research topic is situated in the broader field of aviation security which has received much recognition within academia. Especially after the terrorist attacks of 9/11 literature on this field has expanded. Primarily the focus is put on the government's or private sector's role regarding security screenings and the appraisal of numerous detection technologies (Salter, 2008, p. 243).

2.2.1 Aviation Security

Aviation is a field that faces a diverse variety of security and safety risks. A study on aviation safety has identified eight causes for aviation accidents of international scheduled flights. 'Pilot Error' is the most common cause with 46%, followed by 'Equipment' (29%), 'Weather' (10%) and 'Terrorism/conflict/criminal' (6%). Further listed causes for accidents are 'Seatbelt/turbulence', 'Air traffic control', 'Ground/cabin crew' and 'other aircraft' (Oster Jr., Strong & Zorn, 2013, p. 156-157). Aviation Security Literature not only discusses these risk factors in a generalized manner but also examines them independently in more detail. These risk factors are now complemented by the 'insider threat', that can mostly be ascribed to the category 'Terrorism/conflict/criminal'.

Another focus within aviation security are risk assessments. Tamasi and Demichela (2011)
outline in their paper *Risk assessment techniques for civil aviations security* a collection of quantitative and qualitative methodologies to assess risks in civil aviation's security (p. 892). More specifically is the risk assessment on the security of an airport, with the risk being mainly considered to be an act of terrorism. Security risk management is defined as “an analytical and systematic process, which allows the evaluation of the probability of a threat to result in a negative action towards an infrastructure, people or critical functions of the airport system” (p. 893). With their study Tamasi and Demichela establish a risk assessment framework that supports “the decision making in the design and/or optimization of protection levels for airport security” (p.893-894).

Stewart and Mueller (2013) focus on terrorist attacks in form of “commercial passenger airliners from being commandeered by small bands of terrorists, kept under control for some time, and then crashed into specific targets” (p. 615) in their risk assessment of aviation security. Stressing that terrorism is a type of threat that makes people risk-averse, utility theory includes risk aversion in the decision making process. Risk aversion “arises mostly from the magnitude of the consequences or large losses from a terrorist event”. Applying utility theory presents a possibility to evaluate “risk preferences of the interested parties under choice uncertainty” (p. 616-617).

Commercial aviation is increasingly “a vital sector of contemporary global life” (Salter, 2008, p. 243). Security measures are needed in the industry in order to keep passengers and possibly innocent bystanders safe. Research into the field of aviation security is hence a gainful contribution for society. The analysis of aviation security is done from “a realist, empiricist frame that simply reinforces the state-centric assumptions of power politics” and is perceived “within a national security or policing frame” (p. 245). The relations between state and non-state actors providing security as well as complex relations of threats is thereby neglected (p. 244-246). There is an ongoing debate on incorporating the concept of risk into the field of aviation security and the result of risk being used to justify more security measures (p. 247-253). For the purpose of this research this debate is irrelevant.

Predominantly does the “analysis of aviation security recur[...] back to sovereignty, the state, and the question of security management” (p. 262). The issue is mainly addressed from a US perspective and focuses on airports within the US (Szyliowicz, 2004; Siao, 2017; Black, 2010). Besides the appraisal of vulnerabilities within the industry's security systems, much attention has been given to terrorism and hijackings (Szyliowicz, 2004) and assessments of security risks.

### 2.2.2 Aviation's Insider Threat

In recent years the insider threat in aviation has been receiving increasingly more attention (BaMaun et al., 2016, p. 1-2). With a number of academic articles (Black, 2010; Loffi & Wallace,
2014, Part 1&2; BaMaung et al, 2016) and reports from governments (Krull, 2016; DHS, 2012) having been published, a complex picture of the insider threat can be drawn.

As with many concepts that of the insider threat is one with no unilaterally agreed upon definition (BaMaung et al., 2016, p. 2). IATA defines an insider as “a person who exploits, or has intention to exploit, their role or knowledge for unauthorized purposes. They may be full or part-time permanent employees, individuals on attachment or secondment, contractors, consultants, agency staff or temporary staff” (IATA, 2015, p. 1). The United States Transportation Security Agency (TSA) defines the insider threat as “one or more individuals with access to insider knowledge that allows them to exploit the vulnerabilities of the Nation's transportation system with the intent to cause harm” (DHS, 2012, p. 2).

IATA uses the term 'unauthorized purposes' to describe the actions that are sometimes phrased to cause 'harm'. They include the “sharing of sensitive procedures, attacks on information systems, smuggling goods or people into security restricted areas” (IATA, 2015, p.1). It can further be the sharing of sensitive information or the hijacking of a plane. Personnel in aviation have access to sensitive information, airports, luggage, planes and other fields involving aviation, that can be used to 'harm' the industry (p. 1). The exploitation of an insider's privileges can come in various forms, for example “espionage, insider trading, sabotage, terrorism, embezzlement, extortion, bribery, corruption, and intellectual property theft” (Krull, 2016, p. 4). In other cases the abuse has occurred in form of suicide and workplace violence (p. 4).

KE Krull notices a difference in perspective regarding the definition between the government and the private sector (p. 3). In a similar fashion BaMaung et al. identify a difference between academics' definitions and those of government of the insider threat (p. 2). Generally, the insider is “someone who is entrusted with authorized access, who instead of fulfilling assigned responsibilities, manipulates access to a system to exploit it” (Einwechter, 2002, as cited in BaMaung et al., 2016, p. 2). BaMaung et al. determine the following five overarching themes in the definition of the insider threat: First, trust that is exploited by someone who in the future or present involve himself in insider activity. Second, crucial is access to systems, premises or security critical areas within their employment capacity. Third, a “threat is posed when an insider uses their knowledge of the organization and its systems and/or security procedures to cause harm” (BaMaung et al., 2016, p. 3). Fourth, the insider exploits vulnerabilities in the system and fifth, the intent to exploit the vulnerabilities “and security protocols for commercial, criminal and/or terrorist gain and/or to cause harm” (p. 3).
2.2.3 Aviation's Insider Threat in Academic Literature

A big part of the literature concerning the insider threat in aviation examines the conceptualization of the term 'insider threat' and identifies vulnerabilities of the system for which methodologies to mitigate them are proposed (Loffi & Wallace, 2014; Black, 2010; BaMaung et al., 2016). The attention regarding the vulnerabilities are mostly limited to airports and their security procedures (Black, 2010; Loffi & Wallace, 2014, Part 2).

Krull differentiates between three types of insider threats: The intentional insider “act[s] for self-benefiting purposes without malicious intent” and may cause a risk to security or damage. The unintentional insider can “through action or inaction without malicious intent, cause harm or substantially increase the probability of future serious harm to the organization's confidentiality or integrity”. The malicious insider is motivated by revenge or a personal advantage when intending to directly damage or harm their workplace (p. 4).

The identified driving factors for insider to cause harm mostly overlap with some authors taking a more nuanced approach to them than others. BaMaung et al. see criminal intent by a single person or a group, disgruntlement of staff members and espionage, in recent time especially cyber-espionage, as the main thematic drivers (BaMaung et al., 2016, p. 3-4). Krull states that different factors can be drivers. They include human factors, in form of private stressors such as the death of a friend or divorce; organizational factors, including losing a promotion to a colleague and poor work performance; social; cultural; political and; economic factors. For malicious and intentional insider the circumstances are 'ideal' when one or more of the driving factors in combination with opportunity, intent and motive in form of “revenge, self-benefit, espionage, and intellectual property theft” arise (Krull, 2016, p. 5).

Jon Loffi and Ryan Wallace published a two part essay in 2014 on the insider threat in aviation taking a practice related approach to the issue. In the first part The unmitigated insider threat to aviation (Part 1) a qualitative analysis of risk seven risk factors are determined that are presented by insider threats. Those findings mirror the perception of stakeholders within the aviation industry (Loffi & Wallace, 2014, Part 1, p. 302).

1) Misplace Trust  Even though employees within the aviation industry undergo vetting procedures it is “difficult to identify clear indicators of future employee malfeasance” (p. 293).

2) Crime  It is “the largest and perhaps most unmitigated form of risk” as it entails crimes from theft to fraud. Some positions in the field yield a low salary, whereby
“feelings of entitlement to commit crimes of opportunity to augment income” may arise (p. 302).

3) Terrorism Due to the severe impact an attack could have that is only increased by the sensitive knowledge an insider possess this risk is been given attention (p. 302).

4) Smuggling As smuggling objects into the 'sterile' zone of an airport is difficult due to the security screenings, “organized criminal organizations often recruit insiders to aid in bypassing security measures” (p. 303).

5) Undocumented Workers In this regard specifically, the lack of data based on which the vetting process is made increases the possibility of an insider threat (p. 303).

6) Workplace Violence Its potential is difficult to identify. Additionally, pose dissatisfied employees with access as a critical threat (p. 303).

7) Information Technology With the access to IT systems and sensitive data the cyber threat poses a potential for a new form of terrorism (p. 303-304).

The second part of Loffi and Wallace's (2014) essay The unmitigated insider threat to aviation (Part 2): an analysis of countermeasures focuses on practices to diminish the risk of an insider threat and evaluates the measures' effectiveness (p. 309). Their study identifies “seven categories of internal security countermeasures to detect, mitigate or deter insider threats” (p. 329).

1) Criminal History Record Checks

2) Self-Reporting Requirements

3) Employer Situational Awareness, consisting of Employee Screening, - Behaviour Detection, - Employee Monitoring, - (peer) Reporting

4) Security Threat Assessments

5) Technological Remedies, Situational Awareness Technology and Biometric Access Control

6) Creating Higher-quality Jobs

Alan Black (2010) highlights vulnerabilities of the US commercial aviation system for potential insiders wanting to exploit their position and advocates possible adjustments to securitize these vulnerabilities (p. 1). He raises the concern that employees easily receive access to security sensible areas. As their criminal records may still be clean at the time of their application or they may at a later time in of their employment be extorted or bribed they may also harm the industry. A one time screening of employees is thus not sufficient (p. 3-4). Black proposes different methods to manage the threat: threat assessment methods, surveillance, tracking, 100 percent employee screening, threat profiles and “technological solutions such as biometric systems” (p. 14). His research found that no managing method will eliminate the vulnerabilities. As this is also clear to experts in the field steps toward this goal are inhibited (p. 41).

Krull focuses in his report on the connection of the insider threat and terrorism. He points to the possibility of an insider being recruited by terrorists to harm the industry after that person has worked in aviation for some time or a terrorist may attempt to become an insider themselves (Krull, 2016, p. 1). By analysing previous cases of insider threats related to terrorism Krull identifies “two types of offenders: terrorist members acting on behalf of or in response to an established terrorist organization and lone wolves” (p. 16). As aviation remains a popular target for terrorists because of its international stage and economic value, and insider threats seemingly increase so does the possibility of future terroristic insider threats (p. 30).

The connection between insider threats and terrorism is also drawn in BaMaung et al.'s (2016) essay, as they recognize a terrorist insider's potential impact, if that person holds a position in a critical position. It is stressed that mitigation measures should come holistically. The security management should incorporate a combined effort through cyber, physical and personnel security. Those methods include the identification of changed behaviour or disgruntlement of employees, vetting processes, and raising awareness for these to possibly discourage future threats and “to train staff to understand behaviors of concern in order to protect themselves” (p. 8-12).

Researching literature on the aviation's insider threat has shown that this fairly novel phenomenon is depicted as a risk in academic publications. This subject area can be broadly allocated to the research field of aviation security. There is a general consensus on the conceptualization of insider. An insider is an employee within the aviation industry with access to sensitive areas and knowledge which he/she abuses to cause harm. Next to the terms conceptualization motivators of insider are explored. BaMaung et al (2016) distinguish three broadly categorized drivers, espionage, disgruntlement and criminal intent (p. 3-4) which incorporate themes such as private stressors or economic factors listed by Krull (2016, p. 5). Another focus point within the literature are security
vulnerabilities that can be exploited and possible mitigating measures to counter the insider threat. The viewpoints thereby are mostly airports, or rather their security departments and policy perspectives. Little is written on this issue from a non-american perspective. Missing in the literature is also a detached examination of aviation employees' occupation group such as, mechanics, ground personnel, flight crew. So far an academic approach regarding the insider threat and its positioning within the wider security debate has not been published.

In the following chapter the IRGC's risk governance framework, an approach to assessing and managing risks, will be explained in detail. The framework begins, among other aspects, by establishing the to be analysed problem and earlier signs of the issue being present (IRGC, 2005, p. 8). The above collected information will play a vital role in conducting this step of the framework in chapter 7.
3. Theoretical Framework: The IRGC Risk Governance Framework

This chapter will provide an introduction to the IRGC's risk governance framework. The composition and components of the framework will be detailed, as well as the IRGC's notions on the concept risk. While classical approaches to risk governance involve risk assessment, management, and communication the International Risk Governance Council provides a framework that is more comprehensive. It is said to “serve as a guideline for modern risk governance” (Roodenrijs et al., 2014, p. 1163) as it deals with “both the 'physical' and 'social' dimensions of risk” (Renn, 2008, p. 3). It distinguishes itself from other risk governance approaches by recognizing “the importance of stakeholder inclusion” and differentiating types of risks (Roodenrijs et al., 2014, p. 1163).

The risk governance framework helps to comprehend, analyse and manage risks in five steps which will be discussed below.

In the Pre-assessment phase, the first phase, different perspectives on the risk are discussed and the issue at hand is defined. Indicators for already existing problems, the urgency to act now, involved stakeholders, “scientific/analytical tools and methods that can be used to assess the risks” (Todd, 2011, p.1514), regulatory systems and the organisational capacity of the involved institutions are to be determined in the beginning.

In the next phase, the Risk Appraisal, a scientific risk assessment and a concern assessment are conducted. Thereby it is assessed whether the “risk should be taken and, if so, how the risk can possibly be reduced or contained” (p. 1514). In the risk assessment hazards are identified and estimated, it's exposure predicted and the risk estimated. It is the measuring of its occurrence probability and gathering of measurable factors. Concern assessment comprises economic benefits, public concerns and socio-economic impacts. Herein the risk's perceived consequences and associations with it are analysed. Based on the appraisal a risk is categorized in one of the following four types to help establish a risk management strategy: Simple risks, ones that are proven to be existent by science but is perceived as ambiguous or uncertain by stakeholders, are managed e.g. by introducing new regulations or laws. Complex risks, often affiliated with academics dissent about the issue, can be managed by basing the actions on the most renowned scientific expertise (p. 15-1516). When, due to a lack of scientific clarity, a risk is uncertain, they are often managed by opting for the precautionary principle. Ambiguous risks with differing perspectives on a threat are often countered with a “discourse-based' strategy which seeks to create tolerance and mutual understanding of conflicting views” and will in the end come to a mutual consensus among stakeholders (p. 1517).

The third phase is the Characterization and Evaluation of the risk. It can either be characterized as 'acceptable', where risk reducing steps are perceived as unnecessary, 'tolerable', a risk is taken
because of its benefits but risk reduction measures are taken, or 'intolerable', meaning it is avoided.

If the risk is classified 'intolerable' or 'tolerable' risk management strategies must be applied in the following phase, Management. The strategies include the outline and implementation of measures to mitigate, avoid or retain risks. The measures are furthermore monitored regarding their effectiveness in order to review the management decisions.

The final phase, Communication, is in particular linked to the fourth phase, Management. It gives the public and stakeholders the opportunity to understand the risk and get insights to the issue from different perspectives. The communication should outline the justifications for decisions. People should be able to come to a decision on a risk based on sane and scientific opinions and facts. When successfully done, communication can foster peoples trust in risk management (p. 1515-1517).

In Figure 1 the five phases are set out again including their components which later on will be used for the assessment of the framework's applicability.

| 1. Pre-Assessment | - Problem Framing  
|                   | - Early Warning  
|                   | - Screening  
|                   | - Scientific Conventions  
| 2. Appraisal | **Risk Assessment**  
|              | - Hazard Identification and Estimation  
|              | - Exposure/Vulnerability Assessment  
|              | - Risk Estimation  
|              | **Concern Assessment**  
|              | - Risk Perceptions  
|              | - Social Concerns  
|              | - Socio-Economic Impacts  
| 3. Characterisation and Evaluation | **Characterisation**  
| | - Risk Profile  
| | - Judgement of the Seriousness of Risk  
| | - Conclusion and Risk Reduction Options  
| | **Evaluation**  
| | - Judging Tolerability and Acceptability  
| | - Need for Risk Reduction Measures  
| 4. Management | - Option Generation  
| | - Option Assessment  
| | - Option Evaluation and Selection  
| | - Option Implementation  
| | - Monitoring and feedback  
| 5. Communication | - Communicating Partners  
| | - Type of Shared Information  

**Figure 1:** Five Phases and their Components of the IRGC's Framework (IRGC, 2016)
The framework is not only often referred to in academic literature but also used as a theoretical framework in some cases (Roodenrijs et al., 2014; Renn, 2008; Todd, 2011). Some aspects of the framework have been criticized. One being the lack of a clear 'risk' definition, another being too simple and too complex at the same time, and a lack of internal consistency and of “guidelines for how scientific understanding and knowledge of risk can be balanced against public concerns” (Boholm, Corvellec, Karlsson, 2012, p. 2).

While most people asked about a definition of 'risk' will have the same principle ideas about it, there is no universal interpretation of risk. 'Risk perception' is defined as “the ability of an individual to discern a certain amount of risk” while 'risk tolerance' is “a person's capacity to accept a certain amount of risk” (Inouye, 2014, p. 2). The IRGC also acknowledges that “risk is a mental construct” created through subjective perceptions. It is mainly perception, not facts, that influence human behaviour. Regarding risk perception specific “expectations, ideas, hopes, fears and emotions with activities or events” influence a person’s behaviour (IRGC, 2006, p. 31). This is not to say that such decisions are done irrationally but through the creating of risk images that are evaluated on the basis of evolutionary knowledge. Over time cultural patterns, qualitative evaluation characteristics, influenced these patterns of perception. While risk is traditionally measured by the factors degree of harm and possibility, these qualitative evaluation characteristics go beyond this. Qualitative perception is differentiated into two classes, “situation-related patterns, based on the idiosyncrasies of risky situation” and “risk-related patterns, which are based on the properties of the source of risk” (p. 32). Viewing both classes together their characteristics can be forged into semantic risk patterns. Examples for these are “Risks posing an immediate threat” (e.g. nuclear energy), “Risks dealt with as a blow of fate” (e.g. natural disaster), “Risks presenting a challenge to one's own strength”, “Risk as a gamble” (e.g. stock markets), “Risks as an early indication of insidious danger” (e.g. viruses) (p. 32). People use these patterns to file the experience of a new risk or information on it in an existing pattern. Further do “people tend to stigmatise risk sources that are associated with specific dreadful associations” (p. 32). Often already the suspicion of an object being cancerous can create fear that in return leads to a demand for stricter regulations. Media reports can additionally amplify the public’s perception of risk in ways that are unexplainable by focusing on traditional risk assessment factors, probability and harm. Lastly are emotions and affects factors contributing to people’s perception of a risk. Risk managers need to bare in mind the possibly differing risk perceptions of all involved stakeholders when assessing a risk (IRGC, 2006, p. 32-33).
4. Methodology

In this Chapter the methodological choices that were made are elaborated on and justified. After the thesis' general research design is outlined, the applied data collection methods are explained. Furthermore, are the research's central concepts and their operationalization presented. Lastly, limitations and possible pitfalls of the research are briefly discussed.

4.1 Research Design

The research seeks to establish whether the IRGC's risk governance framework can be applied in the assessment of the insider threat to aviation. For this purpose, the explorative research question, “To what extent can the Risk Governance Framework developed by the International Risk Governance Council be applied in the assessment of the insider threat to commercial aviation?”, will be sought to answer. As discussed above the topic of the insider threat in aviation has not been researched extensively with thus far focusing on the term's conceptualization, identifying weak points within the system and possible mitigation strategies. In academic studies the IRGC's framework has been put to the test in different fields. Yet there is little knowledge about its applicability within the aviation industry. Therefore, the study “works toward more concrete empirical evidence” from a relatively abstract starting point, establishing a deductive approach (Neumann, 2014, p. 69).

In order to put the research question to the test the IRGC framework will be conducted, with the to be analysed risk being insider in aviation, more precisely commercial flight crew. In a first step one airline's risk perception on this menace will be explored. Thereafter will the framework be deployed in a second step of the research process. In a third step the main research question will be answered, through an assessment of the frameworks applicability to the case.

With over hundred airlines worldwide and these companies fear of security information leaks, this study faces two problems. First, airlines will not openly discuss such a security sensitive issue as the insider threat. Secondly, the sheer number of airlines makes the data collection for the scope of a master thesis impossible. Therefore, a qualitative study will be conducted to approach the explorative research question. The research's population are commercial airlines worldwide whereby one airline will serve as a single case-study to represent a fraction of this population. A case-study examines in detail the “case's internal features as well as the surrounding situation”, whereby the structures of the micro level can be linked to the macro level (Neuman, 2014, p. 42). The single-case study's unit of analysis is the airline and the unit of observation is this airline's security department in which the
topic of risk is included.

As mentioned the answering of the research question requires three steps, the first being the exploration of the airline's general risk management and that of the insider threat. The sub questions of the research question are designed to guide this process and will build the base for conducting the risk analysis within the framework of the IRGC. Especially important is the airlines understanding and measuring of risk and the insider threat. It will have to be established how risks are differentiated and categorized. Crucial is the airline's distinction of risk categories. It will have to be established how they can be transferred to the IRGC's categories of acceptable, tolerable and intolerable risks.

Sub Question 1: “How does the airline assess risk?”
Sub Question 2: "Does the airline distinguish different categories of risk in their risk management and if so what are these categories?"
Sub Question 3: “Is the insider threat a recognized threat, if so how is it measured and which category is it attributed to?”

To answer these questions data from the airline has to be collected. After all relevant information from the airline is collected and interpreted the risk assessment with the IRGC framework will be conducted as the second step of the research. Each step of the framework will incorporate knowledge accumulated in the previous assessments. Focus will be put on the first three steps of the framework, Pre-assessment, Appraisal, Evaluation and Characterisation, as the risk assessment is central to the research. Steps four, Management, and five, Communication, will only be discussed briefly.

The third step of the research will then be the evaluation of the framework's applicability in the assessment of the insider threat. For this analysis the concepts and their applicability have to be measured. Paragraph 3.3. Concepts and Operationalization will demonstrate how this will be done.

4.2 Data Collection

Collecting data depends on the accessibility of information. As mentioned, airlines are protective of information regarding their security related procedures. Furthermore, is data on airlines' approach to the insider risk not publicly accessible. In order to nevertheless conduct the research, I approached an airline with a research proposal for the thesis. This air carrier agreed to granting an
insight in their risk management procedure and approach to the insider threat under the condition of concealing their identity. Neither the name of the company, employees or the original department names are mentioned in the thesis. All collected data is documented in the confidential Appendix.

Data is collected through content analysis, observations in their security department and an interview with one of the leading employees within the security department. Viewing the subject from multiple angles increases the research's internal validity (Neumann, 2014 p. 166).

Content Analysis

In a first step to familiarize myself with the company and specifically with its security and risk department, I read descriptions of the security department on the company's intranet portal. This included their organization, duties, and responsibilities. Specifically, relevant for the study are manuals and guidelines for the risk assessment process, which, in parts, were available to me in form of electronic documents. The guideline in particular provides information on risks, their definition and approach to classifying and managing them. Further are publications on the specific topic of insiders and the insider threat used as a source of information regarding the airline's perception of the issue.

After these documents content is evaluated a first picture of the departments operations can be drawn. Content analysis examines all content of communication media. This method of data collection was chosen as it allows one to “discover and document specific features in the content of a large amount of material” (Neuman, 2014, p. 49).

Observation

For a more in depth understanding of the company's perception of risk, their approach to it and the insider threat, I was able to talk to five employees of the security department during a one-day visit. During these meetings the staff members gave a small lecture on their work in general, on the issue of risks, and the insider threat. Additionally, I was able to ask questions on parts of the broader topics risk and the insider threat that were not already covered. The first talk was on the security department organization and general focus points. Then a legal expert gave me insights on policies and legislations regarding air safety and the airline's lobby work. A risk analyst explained the general risk assessment approach used by the airline and also went into detail on the process of the risk assessment of the insider threat. Thereafter I was given an introduction to the company's project that addresses the insider threat. Further I had a conversation with a risk manager whom I was able to question more on the airline's understanding and definitions of risk and the insider.

The information gathered during these conversations were put down in notes and one conversation was recorded and afterwards transcribed. Both the notes and transcript are included in
**Appendix.**

**Interview**

Based on the information gathered through the content analysis and conversations an interview is conducted. The interviewee is the security department's vice director, who also leads the project 'insider threat'. Not all my questions were answered through the content analysis and conversations with employees. The interview was thus an opportunity to answer final questions regarding the airline's risk assessment, procedures underlying this process and their approach to the insider threat. The interview also fostered the airline's understanding of risks and specifically their perception of the insider threat.

The interview is designed as a semi-structured interview. This format is chosen as open-ended questions give the interviewee the possibility to reflect on the discussed topic and give his opinion. It also allows the interviewer to adjust, add, or omit questions to adjust the conversational flow (Magnusson & Marecek, 2015, p. 46-47). The interview is transcribed in full and authorised by the interviewee (see Appendix).

**4.3 Concepts and Operationalization**

To measure the framework's applicability in the assessment of the risk 'insider', concepts central to the framework and the risk *insider threat* need to be operationalized. The framework includes the analysis of the process of a risk's assessment and management. Here the IRGC differentiates between *acceptable risks, tolerable risks and intolerable risks*. These concepts will have to be defined and operationalized as well as the airline's classifications of risks. Indicators for the operationalized concept include aspects of the examined airline's approach to the risk. This is due to the fact that their approach needs to be translated to the framework. The indicators are defined and operationalized below.

**Insider Threat:** An *insider* is a “person who exploits, or has intention to exploit, their role or knowledge for unauthorized purposes. They may be full or part-time permanent employees, individuals on attachment or secondment, contractors, consultants, agency staff or temporary staff” (IATA, 2015, p. 1). The risk of an insider threat is defined in the company's internal publications, e.g. newsletters, regulations, reports, documents containing identified risks.

An employment contract with the airline as flight crew is the basic indicator for an
insider. Surveys on workplace contentment can be an indicator of employee disgruntlement. Internal reports on employees suspected of planning to cause harm can be an indicator and reports on any behavioural change. Financial statements (when employees ask for an internal loan or request financial aid) may help identify an insider threat, as money can be a driver of this risk (Kirkpatrick, 2008). Psychological evaluations can further be used to identify an insider threat. Gathering this information may be done in a working group of the department or in the general risk assessment process of the department (see process).

**Process:** Process is the practice of a risk being assessed and managed. It contains the risk assessment in a qualitative and/or quantitative manner. The policy of the examined airline's process will be written down in a handbook/manual/work instruction. Accordingly, are the standardised procedures outlined in the respective document. Forms can be used to analyse the process as well as digitalised forms in software. Projects dedicated to each defined risk are another indicator. Specific job descriptions of all employees and the hierarchy within the department can further be indicators for the process. Employees' performance evaluations can also be used as indicators as they may outline their specific work.

**Classification:** The airlines differentiation of risks in categories depending on their severity and approach in managing it, defines the concept classification.

First, it shall be established whether risks are classified differently and if so into how many categories. Again, this may be found in a manual/handbook for work instructions. Forms on which the categories are listed can be used as indicators. Similarly, can software databases (steps within it or boxes one can tick) in which risks are typed into be used as indicators. Sub-departments, working groups or projects dedicated to one category are also indicators for classifications. The amount of people working for one project may indicate the importance of that category. The involvement of other departments is another indicator for a category with a higher risk priority.

**Acceptable Risk:** A risk where “any risk reduction step is considered unnecessary”, is defined as an acceptable risk (Todd, 2011, p. 1515).

The definition is found within the IRGC's framework (IRGC, 2005) and is cited in other academic papers (Todd, 2011).
Indicator therefore is the continuation of the status quo without amendments (e.g. new or altered rules, regulations, procedures).

**Tolerable Risk:** A risk is considered *tolerable* when the risk is “pursued because of its benefits and [...] appropriate risk reduction measures” are taken (Todd, 2011, p. 1515). The definition is found within the IRGC's framework and is cited in other academic papers (Todd, 2011).

Risk reduction measures (e.g. regular check-ups on staff through legal records, psychological evaluations, drug tests; implementation of new rules such as “two-persons in cockpit” rule; stricter security searches for crew before boarding an aircraft) are indicators for a *tolerable risk*.

**Intolerable Risk:** If a risk “is so much greater than any benefit that it cannot be taken on”, it is considered to be *intolerable* (Todd, 2011, p. 1515).

The definition is found within the IRGC’s framework and is cited in other academic papers (Todd, 2011).

An indicator are mathematical equations demonstrating that the benefit does not outweigh the risk. The discontinuation of humans working as crew is a further indicator, as well as the suspension of commercial airline flights.

**4.4 Pitfalls and Limitations**

As this research is based on a single case study, generalisations on the IRGC framework's applicability to the entire aviation industry are limited (Neuman, 2014, p. 489). Other airlines may approach risks differently which could show different results when using the same framework to assess the risk of an insider threat.

The data collection is highly dependent on the airlines cooperation. This poses a risk for the execution of the study and its validity. It is possible that the company will not disclose all information on the researched topic as the insider threat is a sensible issue that may affect the company's security. Especially if it is not known that some content is kept unrevealed, the view on an issue may be altered. Ultimately the research's validity would be compromised as a distorted image of the risk assessment is presented.

This research focuses on cockpit and cabin crew as 'insiders'. Generalisations for the
evaluation and characterisation of this risk are limited, as the insider threat originally incorporates more occupational fields within the aviation industry (IATA, 2015).
5. Case Study: The Airline

The following chapter is dedicated to the research's single-case study of the airline's security department. After a brief introduction of the department, their understanding and approach to risks will be presented. Thereafter the airline's view on the insider threat will be depicted as well as the risk's management. The internal risk assessment of the insider will be briefly discussed followed by the internal project insider threat which aims to mitigate the risk of insider.

5.1 The Airline's Safety and Security Department

The airline's Safety and Security Department is composed of three sub-departments, namely Safety Operation, Aviation Security, and Company Security (Appendix, Figure F & Figure A) The sub-department Safety Operation is dedicated to defining common safety standards that are to be implemented throughout the airline (Appendix, Figure G). Within the Aviation Security department issues related to enabling a secure execution of flights are addressed. The areas of responsibilities include lobbying and the subsequent compliance to regulations, services related to aviation security such as crisis management and monitoring of conflict areas, and risk management. The latter incorporates the analysis of countries' security situations worldwide, audits, monitoring overflights of conflict areas, mitigating risks and crises (Appendix, Figure H&I). The sub-department Company Security addresses security concerns that are related to the company's entire operations. It's four purviews are: first, Executive and Event Protection, the protection of the board members and big company events; second, Intelligence and Investigation, the prevention of white-collar crime and investigations in suspected cases of corporate espionage or other cases that may harm the business integrity; third, Information Protection and Business Risk Management which mainly addresses cyber security; and fourth, Employee and Asset Protection, which entails property protection, consultations for duty travellers and expats, and threat management (Appendix, Figure J&K).

The risk of an insider threat is managed within the Company Security department and is considered part of the threat management.
5.2 Understanding and Approach of Risks

5.2.1 Definitions and Understandings

It is in the nature of an airline to entail risks that are not only industry-sector specific but also ones stemming from the fiscal and macroeconomic field (Appendix, Guideline, p. 1-2). A risk thus can come in various forms, for example fluctuation in fuel prices or currency exchange rates, political unrest, terrorism or a financial crisis. An ever-changing environment can also bare chances for a corporation. The concept risk and chances are viewed as their respective counterparts. Both concepts are mostly connected to financial aspects, which is reflected in their internal definitions: “The term risk […] is defined as a negative […] deviation from a forecast or target value”. 'Opportunity' is a positive “deviation from a forecast or targeted value” (p. 3).

While generally risks are connected to economics and are seen as quantifiable, security related risks are difficult to measure, particularly in monetary terms. When considering security related risks the transition from an issue into a risk is a gradual process whereby the pain threshold for this transition depends, to some extent, on the risk manager's gut feeling (Appendix, Conversation, p. 15) and experience. In this process of constituting how a risk is defined, risk authorities are involved by laying out a legal framework with regulations. Generally, the company strives for a pro-active approach towards risk, in order to mitigate risks as early as possible (Appendix, Guideline, p. 3).

The airline has established a guiding principle concerning risks that is evident across their work: the closer a threat comes to an aircraft the bigger the risk (Appendix, Conversation, p. 81). This idea is also reflected in the airline's worst-case scenario. As the most severe outcome of a risk, a hull loss, or total loss, is defined. This implies “Multiple fatalities and/or permanent disabilities with serious illness or health impair-ments” of passengers and a total loss of an aircraft (Appendix, Figure D).

5.2.2 The Risk Management Guideline

Due to the fierce competition on the aviation market, it is important for the airline to identify risks as soon as possible in order to appraise and mitigate them. At the same time airlines often see themselves in the spotlight being publicly critiqued. This is seen as a further reason to mitigate risks and possibly protect themselves from negative publicity. For this purpose, a risk management guideline with a systematic approach to risks has been developed. Mitigating risks early on will not only make the airline less vulnerable, it also presents them with the opportunity to create a competitive advantage over others. As mistakes are always connected to financial losses it is a further reason for
them to mitigate risks and learn from those that were unavoidable.

This regulating system identifies potential opportunities and risks and subsequently manages them whereby realizing opportunities. The main aim of the risk management is “the pursuit of an optimized decision quality and planning accuracy as well as a preventive preparation and management of imaginable risks” (Appendix, Guideline, p. 1). The airline's risk management is closely associated with its economic goals while “reducing the volatility of earnings” (p. 2). All the company's departments are obliged to apply the guideline's regulations (p. 1-3). The risk management's organization is an interwoven construct that includes the cooperation and communication of the concerned departments and the executive board. Risks are managed by the affected departments according to the guideline and with the aid of an appointed coordinator (p. 4-8).

Five phases constitute the risk management process: risk identification, risk assessment, risk management and monitoring, risk reporting, and integration of risk management into general management processes. Each phase will be detailed below.

**Identification**

In a first step both present and potential future risks are identified, as well as risk drivers. A risk catalogue that is continuously updated serves as a compendium when determining risks. Every identified risk has to be catalogued in this document (p. 8). As the industry is in constant change which is influenced by many factors, risks are to be identified on a quarterly basis. This can be done through a creative approach, analysing scenarios or brainstorming, or structured methods, reviewing the catalogue, checklists and interviews.

**Assessment**

The second step is the risk assessment in form of a quantitative and qualitative evaluation (p. 9). The required methods therefor are designed by the sub department Aviation Security (p. 5-6). A risk is monetarily examined to assess whether it crosses the “eligibility limit, that is to say the lowest threshold of the extent of damage” (p. 9). If this is the case, the risk needs to be monitored in the following phases of the risk management. Predominantly should risks be assessed quantitatively with the help of empirical figures or other objective criteria. If the assessing employee finds the risk is not quantifiable, a qualitative assessment should be conducted. Risks are divided into three classifications, distribution risks, event risks and qualitative risks, before they are assessed (p. 9-10).

Distribution risks are ones that are certain to occur, but the damage of their occurrence is ambiguous. The difference between the risks worst case, expected case and best case amount to the risk value. This risk value can be attributed to an A-, B-, or C-Risk (Appendix, Implementation, p. 7). Within each of the three risk groups a classification is made into A-, B-, C-, and in the case of event
and qualitative risk also D-Risks. Starting at a D-Risk the classifications are equated in ascending order. These categories represent marginals of monetary value caused by the damage of a risk (Appendix, Guideline, p. 10-11). Distribution risks are considered in the company's planning, due to their certainty to occur. Examples for this type of risks are fluctuating exchange rates and fuel prices.

**Occurrence Probability**

<table>
<thead>
<tr>
<th>100.00%</th>
<th>C</th>
<th>C</th>
<th>B</th>
<th>B</th>
<th>A</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt;= M* 1</td>
<td>&gt;= M* 2</td>
<td>&gt;= M* 3</td>
<td>&gt;= M* 4</td>
<td>&gt;= M* 5</td>
<td></td>
</tr>
</tbody>
</table>

(\*M = Marginal)

**Figure 2:** Distribution Risk Classes

(Appendix, Implementation, p. 7).

Event risks are risks of an incident that can, but do not necessarily occur, such as an airspace closure. These risks are quantitatively assessed, always considering a one-year time frame. If the risk's probability is 50% or higher, the event risk is relevant for the airline's planning.

**Occurrence Probability**

<table>
<thead>
<tr>
<th>&gt;= 50%</th>
<th>C</th>
<th>C</th>
<th>B</th>
<th>B</th>
<th>A</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt;= 30% - &lt;50%</td>
<td>D</td>
<td>C</td>
<td>B</td>
<td>B</td>
<td>A</td>
</tr>
<tr>
<td>&gt;= 20% - &lt;30%</td>
<td>D</td>
<td>C</td>
<td>C</td>
<td>B</td>
<td>A</td>
</tr>
<tr>
<td>&gt;= 10% - &lt;20%</td>
<td>D</td>
<td>D</td>
<td>C</td>
<td>B</td>
<td>A</td>
</tr>
<tr>
<td>&gt;= 2% - &lt;10%</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>B</td>
<td>A</td>
</tr>
</tbody>
</table>

| >= M* 1 | >= M* 2 | >= M* 3 | >= M* 4 | >= M* 5 |

(\*M = Marginal)

**Figure 3:** Event Risk Classes

(Appendix, Implementation, p. 8)

Qualitative risks are unable to be evaluated in monetary terms, but nevertheless need to be evaluated. Therefore they are assessed qualitatively. More specifically are they classified according to their significance, or impact, level and indication, or probability, level. The latter describes the density of information existent, while the significance level describes the impact. Figure 4 depicts a map with
which qualitative risks are categorized into an A-, B-, C-, and D-Risk. These types of risks do not affect the airline's annual planning due to “the lack of relevant information” on them (p. 9). Examples of qualitative risks are crises, wars, cyber risks, crises related to airline operations (Appendix, Figure L)

<table>
<thead>
<tr>
<th>Indication</th>
<th>Figure 4: Qualitative Risk Classes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(Appendix, Implementation, p. 9)</td>
</tr>
</tbody>
</table>

**Risk Management and Monitoring**

After the risk is assessed suitable mitigating instruments are defined and implemented in the third step. The objective of the measures is a proactive approach to the risk. Risk correlations need to be considered in this phase of the risk management. As the risks are continuously monitored, changes are recognized in a timely manner and can lead to amendments to the risk's management. Further do the mitigating measures' cost-benefit ratio have to be established (Appendix, Guideline, p. 11-12).

**Risk Reporting**

The fourth phase is the creation of a risk report, containing current opportunities and risks. It is created quarterly and imparted to the executive board. It composes evaluations compiled by the risk involved business segments. For distribution risks it needs to be established to what extent they “are already considered in the earnings forecast” and to what extent they may lead to a deviation from the expected earnings (p. 12). Top event risks and qualitative risks need to be listed as well as the corresponding management measures and effectiveness. Changes that lead to a modified appraisal need to further be listed. Newly identified Type A risks need to be reported to the executive board as well as the risk management officer through ad hoc notifications (p. 12).
Integration of Risk Management into the Management Processes

The results of the risk identification, assessment, analysis and management are documented in reports and presented at the annual company meeting. The data is then used to plan the risk controlling within the strategic operational corporate planning. Not only the responsibilities and processes enabling “an effective and efficient risk controlling are defined” in the operational corporate planning but also the corresponding budget (p. 13).

5.3 The Airline's Insider Threat

5.3.1 Definition

Once the risk of an insider was identified by the airline a definition for this concept had to be established that is tailored to the airline. As a result the insider is internally defined as “a person who abuses its professional position or tries [...] to commit unallowed actions that influence the security or that may cause a significant damage to [...] [the company]. Insider can be employees, temporarily employed persons, interns, consultants, suppliers or other persons that are related with [...] [the company]” (Appendix, Figure B).

The term 'unallowed actions' generally refers to actions that can cause harm. When someone with a mandated assignment of tasks sways from his job description and has the goal to cause harm to the corporation or individuals, the airline speaks of 'unallowed actions'. The intent hereby is of importance, as only someone with a malicious intent is considered to be an insider. Unintentional actions that lead to damage are regarded as mistakes. A damage caused by an insider is defined to be 'significant', when this damage can be classified as significant within the risk matrix (see Figure 2).

It is specified that the risk is constricted to insiders whose motives are of a radical or terroristic nature. The focus on these two drivers is connected with the security department's guiding principal: the closer a threat is to the aircraft, the bigger the risk. Terrorism and motives stemming from radicalization are likely to include harming people and the corporation. Thereby a life and death scenario is more likely than for example an insider driven by an economic motive (Appendix, Interview, p. 92-93).

The guiding principle of a threats proximity to the aircraft influencing the risk is also reflected in the risk matrix for the insider threat as demonstrated in Figure 5. This matrix is based on the general risk matrix of qualitative risks and shows a taxonomy with which security standards for potential insiders will be established in the future. The X-axis indicates an insider's impact on the airline's infrastructure when conducting unallowed actions. 'Public' spaces are ones that can be accessed by
anyone. 'Non-critical infrastructure' points are sites that are not public but damage there would be minimal. 'Non-flight ops critical Infrastructure' implies areas that are not directly linked to flight operations but where done harm still has severe consequences. The 'supply chain' includes areas that work independently from the airline or only the flight operations, but their end product is in direct contact with the plane, e.g. catering. 'Flight operations' includes all infrastructure areas that are directly involved in the execution of a flight. The Y-axis indicates the probability of an employee abusing his position to cause harm (Appendix, Figure C&D). This probability is mainly determined by a country's terrorism risk level. Further can external factors, such as actual threats that are known, as well as internal factors, staff ratio, fluctuation, age structure and the percentage of men working there, influence the probability. The intersection of a probability and impact is the security standard that needs to be implemented. 'A' suggests an extreme, 'B' a high, 'C' a medium and 'D' a low security standard (Appendix, Conversation, p. 88).

<table>
<thead>
<tr>
<th>Probability</th>
<th>Public</th>
<th>Non-critical Infrastructure</th>
<th>Non-Flight Ops* Critical Infrastructure</th>
<th>Supply Chain</th>
<th>Flight Ops*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very high</td>
<td>C</td>
<td>C</td>
<td>B</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>High</td>
<td>D</td>
<td>C</td>
<td>B</td>
<td>B</td>
<td>A</td>
</tr>
<tr>
<td>Medium</td>
<td>D</td>
<td>C</td>
<td>C</td>
<td>B</td>
<td>A</td>
</tr>
<tr>
<td>Low</td>
<td>D</td>
<td>D</td>
<td>C</td>
<td>B</td>
<td>A</td>
</tr>
<tr>
<td>Very Low</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>B</td>
<td>A</td>
</tr>
</tbody>
</table>

A = Security Standard A  
B = Security Standard B  
C = Security Standard C  
D = Security Standard D  
*Ops=Operations

**Figure 5**: Insider Threat Matrix

### 5.3.2 Evaluation of Insider Threat based on Risk Management Guideline

In 2016 the insider threat was identified as a risk by the airline (Appendix, Conversation, p. 86). Prior was the topic touched upon internally within the context of the airline's threat management programme (see Chapter 5.4). In the risk catalogue 'staff' has already been listed as well (Appendix,
Implementation, p. 5) but the issue of insider was not explicitly identified as a risk until then. By that time incidents and attacks worldwide in the aviation industry involving insiders as offenders accumulated. This consequently became a topic on aviation conferences and led to its rise on the company's security agenda (Appendix, Conversation, p. 86). Furthermore, was the topic brought to the airline's attention by outside panels and law enforcement (Appendix, Interview, p. 91). As a result, the project 'Insider Threat' was launched with the goal to create a holistic approach for this risk. In the beginning a pre-project was conducted in which the basis for the project was laid out, a definition for the term insider, what risks can be deduced from the original risk, 'staff', and what countermeasures will have to be implemented (p. 97).

The risk assessment of the insider threat is done solely through a qualitative approach, as it is classified as a qualitative risk (Appendix, Conversation, p. 75). The airline does not have a database with incidents caused by insiders internally or on a global scale. On the one hand is the collection of such data illegal without seeking the board's approval prior. Having this type of database is not necessarily a goal for the company. They only see it as necessary to be aware of the fact that the transformation from an employee into an insider is a gradual process and this process needs to be documented. For this purpose, it is the goal to buy an appropriate tool (Appendix, Interview, p. 96-97). On the other hand, a quantitative approach is not followed, as it is believed that past incidents are unable to predict the future (Appendix, Conversation, p. 75-76). For the risk insider a separate matrix was developed (see Figure 5) based on the qualitative risk matrix, as it is difficult to generally attribute the versatile risk insider to one risk classification. As the caused harm of an insider attack per definition needs to be “significant” (Appendix, Interview, p. 93), the insider threat would be classified at least as a B-Risk.

Management and monitoring of the insider threat are documented in the insider threat guideline that will be approved by the board in 2018 and then published. This guideline is the result of the project Insider Threat. As all qualitative risks, the risk of an insider needs to be listed in the regular risk report. The integration of the risk into the risk management has begun. A reflection hereon is at this early stage not possible.

5. 4 Project Insider Threat

The project insider threat was launched in 2016 with the goal of creating a holistic approach to the risk applied throughout the airline (Appendix, Figure E). It also aims to install future policies
that will define standards for the established areas of action of the project (Appendix, Interview, p. 90). The project is incorporated in the Company Security's Employee and Asset Protection (Appendix, Figure K). These areas of action are *Background Checks and Recruiting, Access Controls, Security Awareness, Third-Party Management, Threat Management.*

Ideally a potential perpetrator is not given the opportunity to become an insider. For this purpose, measures for *Background Checks and Recruiting* are implemented. Background checks are already mandatory, new are integrity tests that are added to the recruiting process to identify potential insider (Appendix, Interview p. 90).

In the course of the project it was decided that stricter *Access Controls* will be conducted. Tests for explosive substances are now part of the security check of employees, when entering secured areas. Further are all properties of the airline and of third-party service providers reevaluated regarding their access (p. 97-98).

To generate *Security Awareness* the internal communication of the insider threat is increased by creating new content for the airline's intranet. Employees in a management position are given a training on the insider threat and learn how to make a first assessment of a potential insider and where to report this (Appendix, Conversation, p. 86).

Service providers working for the airline built another area of action, the *Third-Party Management*. Where the airline has a direct influence on service providers they already demand a minimum standard which is controlled and audited. The airline is currently developing a contract clause that requires service providers worldwide to fulfil certain standards similar to those of the airline. Additionally, the airline lobbies for new standard contracts that include the above-mentioned security measures (Appendix, Interview, p. 100).

The area of *Threat Management* can be perceived as the one incorporating all other areas of action (p. 95). It includes the subject areas Radicalisation, Stalking, Violence at the Workplace and Threats (Appendix, Conversation, p. 77). Its goal is to identify possible threats, including ones of radicalised or terroristic motivated insider, before any harm is done through the reporting of suspicions in one central department (p. 81). The threat management is divided into five phases.

1. A threat is identified through a cumulation of incidents by a person that are reported to the security department. Whether a case is pursued depends on the department and their gut feeling, as there is no defined starting point of a situation that is said to be a threat.
2. In an initial assessment of the case two models are used to assess the severity of the threat.
3. Based on the models' results it is decided whether the case is pursued and whether aid by external institutions is needed.
4. Then further information is collected and assessed.
5. The management of a case is conducted intuitively, and measures are weighed against one another (p. 77-87).

When the case of an insider is identified hard facts about the suspect need to be established. This information is always gathered with the help of the department in which the (suspected) insider works and human resources. Depending on the case, internally the security department, social-medical counsel, medical department and legal department may be involved. The case is always discussed with these entities in an anonymised manner. In the case of the medical department they will contact the security department for advice on a case, whereas the security department will ask the other departments for assistance. Help for cases is also sought externally from law enforcement, prosecution, expert groups and psychological services (Appendix, Interview, p. 99-100).

Already during the project were countermeasures for the insider threat implemented, as some departments had independently started to counter the risk. This was for instance the case for the field recruiting and background checks. The mentioned integrity tests were quickly applied as the responsible department was already evaluating such tests. Similarly, were measures in the area of access controls rapidly incorporated, such as explosive trace detection tests (p. 97-98).

5.5 Crew Members as Insider

The airline's definition of insider is written to potentially include any company or third-party employee, also flight crew. A differentiation of insider regarding their working environment is indirectly given through the Insider Threat Matrix and differentiation of impact level (see Figure 5). As crews' work area are flight operations they are automatically ascribed to the highest security level, regardless of the probability. This classification is again a derivation of the department's guiding principle of a threats proximity to the aircraft. Through legislations the airline is also obliged to differentiate between employees as air law dictates for instance different background checks and access controls for airline employee's depending on their work space and job description (Appendix, Interview, p. 94).

Even though a differentiation of personnel regarding the insider threat is done, crew members are not viewed separately. In the course of the project insider threat several amendments to existing procedures were introduced to mitigate the risk. For flight crew the main new measures are those in the field of recruiting. Due to their job description they already need to meet the highest security standards. This entails stricter background checks and more complex access controls to their
workplace then for employees not working in direct proximity of flight operations. These access controls are catholic as everyone undergoes a full control of their person, as well as their luggage, before entering an aircraft (p. 90-92).

While those involved in the flight operations have more possibilities to harm the airline, the potential for these individuals to act on these possibilities is not higher. Further, is the process of becoming a crew member much more complex and protracted than gaining access in other areas of an airline. The training to become a commercial pilot takes approximately three years and becoming a flight attendant about three months. It is thus a lengthy process involving background checks and psychological evaluations that may expose a malicious applicant before being employed. For the airline crew members are hence not a special focus within the risk insider threat (Appendix, Conversation, p. 86).
6. Hitherto Conclusions

6.1 Answers to Sub Research Questions

The first research sub question aims to understand how the airline assesses risks. The case study has shown that the studied airline has a comprehensive and multi-layered system with which they assess risks. Risks are assessed by the concerned departments with the help of the company's risk management guideline. After a risk is identified the next step is its assessment. The risk is attributed to one of the three different risk classes: distribution risks, ones that are certain to occur, event risks, ones that have a probability lower than 100% to occur but higher than 0%, or qualitative risks, ones that cannot be conveyed in monetary terms. Every identified risk is then evaluated qualitatively and quantitatively, unless the assessing employee believes the risk not to be quantified (Appendix, Guideline, p. 8-9).

Once the risk is attributed to a risk class and is assessed the airline assigns the risk to one of four risk categories (A-, B-, C-, D-Risk) in order to prioritize them. Thus, the second sub question can be affirmed. The categories in which risks are classified represent the marginal for the damage of a risk. A D-Risk has the lowest marginal while an A-Risk has the highest (p. 9-11). The classification of a risk has no indication about the to be taken management measures. Instead it is an indicator for the gravity of financial losses connected to a risk.

The insider threat is a recognized risk by the assessed airline, affirming also the third research sub question. This risk is a qualitative risk according to the company's own guideline. As mentioned, it was decided to create a separate risk matrix for this specific risk, as it can occur in diverse forms and it is difficult to attribute it in general to one risk class. This Insider Threat Matrix measures the risk through two indicators, the impacts location and the probability of it happening. The measurement leads to a security standard that needs to be fulfilled for this risk (Appendix, Figure C).

6.2 Reflection on the Case Study

It is evident that risks are a topic of high priority for the airline. The company not only has developed an intricate guideline for their risk management, it also involves a complexity of people, demonstrating that risks are taken seriously. The airline's definition of risks, “a negative […] deviation from a forecast or target value” (Appendix, Guideline, p. 3), mirrors the company's strive for economic success. Risks are translated into monetary value by weighing the probability of its occurrence with its potential damage. As some risks, especially security related ones, are not directly quantifiable, the firm takes a slightly different approach to these qualitative risks (Appendix,
Implementation p. 7-9). The research for the case study has shown that the insider threat is indeed a recognized risk within the airline. The risk has been recognized, classified and in the course of a project new management and mitigation strategies have been established. In this process the insider threat was defined as a qualitative risk and was not quantified in any way.

An insider is defined by the airline as “a person who abuses its professional position or tries [...] to commit unallowed actions that influence the security or that may cause a significant damage to [...] [the company]. Insider can be employees, temporarily employed persons, interns, consultants, suppliers or other persons that are related with [...] [the company]” (Appendix, Figure B). A closer look at this definition shows that it is kept broad with room for interpretation. This leaves the evaluators of potential insider the possibility to decide each case individually and let their gut feeling be part of the process. The five general themes in insider definitions identified by BaMaung et al. are mostly found in the airline definition. 'Violation of trust' (BaMaung et al., 2016, p. 3) is not explicitly mentioned in the firm's definition. The phrase “abuses its professional position or ties” (Appendix, Figure B) hints at the theme of trust, as employees are trusted with duties they are expected to fulfil accordingly. The theme of 'access' to sensitive areas is also not directly included but implied again through an employee's area of responsibility. A 'threat causing harm' (BaMaung et al., 2016, p. 3) is directly mentioned with the phrase “to commit unallowed actions that influence the security or that may cause a significant damage” (Appendix, Figure B). Not included in the definition is the 'exploitation of vulnerabilities', as well as the 'intent' (BaMaung et al., 2016, p. 3). The latter is crucial to the airline, when labelling a perpetrator as an insider. If damage is caused unintentionally, the airline speaks of an accident. Even though the 'intent' is not included in the definition, in practice it is considered.

When the airline speaks of insider they restrict this definition to persons who's motive stem from a radicalisation or are of a terroristic nature (Appendix, Interview, p. 90-91). In the literature on the phenomenon a wider spectrum of drivers is enumerated. They range from personal disgruntlement, over criminal intent and terrorism to espionage (Krull, 2016, p. 5; BaMaung et al., 2016, p. 3-4). The airline's limitation to these two motives are explained in two ways. First, they believe that the damage an insider with a terroristic motive is likely to lead to greater damage than the damage resulting from a monetary motivation. Especially as terroristic damage is more likely to include the loss of life. Second, the airline differentiates between a 'security' and 'safety' department and their addressed tasks and issues reflect the discrepancy of the terms. As the issue of the insider is handled by the security department, the motives of the insider reflect the department's security perspective (Appendix, Interview, p. 90-91).

A differentiation of insider depending on the personnel's job description and work area is given through the Insider Threat Matrix. As an airline incorporates such a wide range of tasks it would be
impossible to extend the categories to the number of job groups. Using the security department's guiding principle for the risk of insider thus seems logical. Including everyone who directly touches upon the flight operation process, not only crew, in the highest security standard seems a reasonable decision.

Overall, it can be said that the airline perceives the insider threat as a risk to their business and measures are being implemented to reduce this risk. The importance of the issue can especially be demonstrated through the existence of an entire project dedicated to the insider threat. This project has been in the works for two years (Appendix, Conversation, p. 74) and involves a number of people (Appendix, Interview, p. 97). This alone is a costly process and with the implementation of integrity tests and awareness training even more costs are generated. The air carrier's willingness to invest time, manpower and money in the risk indicates it is an important threat that is hoped to be reduced. In the case of an insider attack it can be shown that measures were taken beforehand. Their assessment of the risk was fact based, culture and emotions seem not to have been actively considered in the assessment process. Ascribing the insider to one of the semantic patterns of risk perception referred to by the IRGC is difficult. Most fitting is the perception of 'risk as a gamble', as the employment of trustworthy personnel is a gamble (IRGC, 2006, 32).

Flight crew is not perceived as a particularly risky occupational category within the group of insider (Appendix, Implementation, p. 86). While it is true that there is no correlation between an employee’s possibility to cause harm and the probability of the harm's execution, there are aspects to flight crew as insider that may be underestimated. Contrary to ground personnel, they have unsupervised control over an aircraft for the duration of a flight. While going to the lengths of acquiring a commercial pilot license for the purpose of becoming an insider is unlikely, the much shorter time needed to become a cabin crew member may be attractive to perpetrators. On short haul flights with fewer flight attendants on board a perpetrator could easily act undisturbed. Antipodal to an office environment, crew does not work with the same group of people on a regular basis. Changing behaviour or attitudes often seen as indicators for insider would likely go unnoticed in this environment. An incident in an aircraft caused by its own crew would surely generate great public attention, as ultimately an airlines figurehead are their planes and crew. Particularly for terrorists would this scenario of attack be a triumph that will be mediated on a global scale. The existing and planned risk mitigating measures are and will no doubt aide in reducing the risk of an insider attack. But 100% security can never be warranted and 'where there is a will, there is a way'. This is to say that flight crew should not be neglected as potential insider.
7. The IRGC Framework Applied

In this chapter the IRGC's framework will be applied to assess the risk of commercial crew members as insider to the aviation industry. The perspective for the assessment will be from an outsider’s point of view looking onto the environment in which the insider threat is situated. As the terminology for the field of risk and the insider threat has been discussed in the literature review and theoretical framework definitions will mostly not be repeated, nor will the IRGC framework's steps be outlined again. The framework's structure is detailed in chapter 3. Most information used to conduct the framework stem from the literature review and knowledge obtained through the case study. The researched airline's perception of the risk is used in a generalized manner to represent the perception of airlines worldwide. After conducting the framework, it's applicability will be assessed.

7.1 Pre-Assessment

One of the early publicly documented cases of an insider harming the aviation industry was the 1998 Air China incident. In the following years a number of insider cases in the aviation industry became public (Loffi & Wallace, Part 2, 2014, p. 307-309). It is likely that there are cases that have not been disclosed to the public. It is unclear to what extent these early incidents were seen as warning signs of the emergence of the phenomenon insider. Black (2010) identified the first publicized report on the industry's awareness of the insider threat to be a U.S. Homeland Security Assessment by the Federal Bureau of Investigation and Department of Homeland Security in 2007. The following year the TSA warned in an information bulletin about insiders, and again in 2009 (p. 13-14). As a representative of the majority of commercial airlines worldwide IATA publicly ushered concern about the insider threat in 2015 (IATA, 2015). Academics also warned about the phenomenon. Black (2010) was among the first to academically contribute hereto, followed by, among others, Wallace and Loffi (2014, Part 1&2), Krull (2016) and BaMaung et al. (2018). Past incidents, warnings by governmental institutions, and the prediction that insider cases are likely to increase in the future (Krull, 2016, p. 30) demonstrates that the insider threat is a recognized hazard that demands action.

While there seems to be a general consent about what constitutes the insider threat, it is conceptualized slightly different by involved stakeholders. The insider threat to commercial aviations bears a number of stakeholders, including government institutions concerned with transportation, commercial airlines, representatives of the airlines (e.g. IATA), commercial airports, and the public who potentially are flight passengers.
Public perception of the insider threat is important as it is “a driver for security activities performed at airports” (Black, 2010, p. 22) and likely influences the other stakeholders. Especially airlines need to consider the public perception as they generate their proceeds. In 2017 approximately “4.1 billion passengers were carried by the aviation industry on scheduled services” (ICAO, 2018). This number does not take into account connecting flights or passengers travelling more than once. Nevertheless, does the number demonstrate that the hazard potentially influences a great number of people. While there are no specific studies found on the public's perception of the insider threat, a majority of the flying public will have become aware of the insider threat through media reports on past incidents. Particularly the crash of the Germanwings flight in 2015 generated public attention globally for the potential harm crew members can cause.

Definitions on the insider threat differ in regard to what constitutes an insider. The U.S. Government for instance sees an insider as an aviation employee who knowingly or unknowingly harms the country's security. The private sector in contrast omits the 'unwitting' factor and considers the harm from an insider to damage “the organization, or an unauthorized act that benefits the individual” (Greitzer et al., as cited in Krull, 2016, p. 3-4). This mostly correlates with the findings from the case study. The examined airline also only considers someone who intentionally causes harm to be an insider (Appendix, Interview, p. 91). What links the industry's stakeholder is their perception of the insider threat as a risk.

The spectrum of aviation insiders is complex and, as introductorily mentioned, difficult to assess as one risk. As a frame for this assessment the hazard of insider will hence be confined to commercial cabin and cockpit crew. Drawing on the various previously cited definitions the insider in this context is defined as an employee of a commercial airline who's occupation (part- or full-time) is being a flight crew. The employee (has the intention to) wittingly exploit his insight or role for unauthorized purposes to cause harm. In order to bundle the motives behind such an action BaMaung et al.'s (2016) thematic factors are adopted: espionage, criminal intent (including terrorism), and disgruntlement (p. 3-4).

The previously studied airline is currently putting into place methods that aim to mitigate the risk of an insider, both during the hiring process and for suspected cases (Appendix, Interview, p. 95-96). As airlines come together to exchange information on the current situation of the industry, follow the news about competitor's incidents etc., it can be assumed that all airlines are aware of the risk. In order to protect themselves from criticism of not having acted on this knowledge, it can further be assumed that many will have installed similar mitigating measures. The UN agency International Civil Aviation Agency (ICAO) works with the industry's groups to “ensure that their local civil aviation operations and regulations conform to global norms” (ICAO, n.d.a). One of this global norms
states: “Each contracting State shall ensure that background checks are conducted on persons other than passengers granted unescorted access to security restricted areas of the airport prior to granting access to security restricted areas” (Appendix, Figure M). As a result, are airlines in the U.S. obliged by the Federal Aviation Administration regulation that background vetting of applicants are conducted. If the applicant has been charged with crimes related to aviation, treason, murder and more he will not be signed (Aviation Personnel, n.d.). Similarly, are air carriers registered in the EU obliged to conduct security background checks for future employees. Once a person is under contract this background check needs to be renewed at least every five years (European Commission, 2015).

These regulations can prevent potential perpetrators from becoming insider and may identify those working for an airline. If an insider is not caught through the background checks and is already an airline employee, it is difficult in many countries with strict labour laws to fire a possible perpetrator without clear evidence of his intentions.

As outlined in the literature review there are quantitative and qualitative approaches to assessing risk in aviation security. For a quantitative assessment data is needed on the frequency probability of such events (Tamasi & Demichela, 2011, p. 892-893). As there is no publicly accessible database a quantification of the threat is not possible. Therefor a qualitative risk assessment to appraise the risk of an insider threat cannot to be applied.

7.2 Appraisal

The IRGC considers both factual dimensions of the risk and socio-cultural dimensions to be important to draw adequate conclusions about the risk (IRGC, 2006, p. 12). The Appraisal is therefor divided into two parts. The scientific risk assessment focuses on measurable factors, whereas, the concern assessment focuses on stakeholder perceptions and emotions associated with the risk.

Scientific Risk Assessment

The damage stemming from a crew member abusing his knowledge and power through his occupation can vary immensely. It may range from selling information on passengers or procedures, to material (hull) losses, to the loss of human life. Any damage will be related to financial and reputation losses to the respective airline and possibly other stakeholders. As there is not one defining cause to the threat (BaMaung et al., 2016, p. 3-4) and no single effect variation, a clear cause-effect relationship cannot be established. What can be established is that the cause for an attack, in its broadest definable term, is discontent. The resulting effect of an unauthorized action driven by this
discontent can broadly be described as harming to the aviation environment.

An insider attack can particularly impair the affected airline's reputation and may cause financial losses. To what extent the damage is reversible depends on factors, such as media attention, the death toll and an effective crisis management. Consequences may also be felt by governments facing criticism for an inadequate regulatory framework. Due to the aviation industry's affinity to the media, an insider case is prone to raise international attention. If a leak of information is publicized this may cause a financial setback to a carrier.

Through the exposure of insider cases, previously used security holes used to cause harm can be closed. From successful insider attacks a secondary opportunity is the learning effect. It is further possible that responsible stakeholders show a bigger willingness to change the current status quo, possibly due to pressure from the public.

Calculating the probability of the occurrence of an insider causing harm is next to impossible, due to a lack of accessible data. Academics believe insider attacks will occur in the future and as they have occurred in the past (Krull, 2016, p. 30) their probability can be said to be larger than 0%.

**Concern Assessment**

While there are no studies on the public's perception of the insider threat to aviation, deductions can be made based on more general studies. In the last years air travel has become significantly safer. Nevertheless, aviation still has the stigma of being a 'risky' means of transportation. Between 10% and 40% of air travellers have varying degrees of flight phobia (Bor, 2007, p. 209). Studies on the public's risk perception of air travel show large discrepancies in their results. These discrepancies can be explained by differing dimensions in the studies. Backer-Grøndahl and Fyhri, (2009) found that people's ranking of transportation modes is intuitive. Comparing planes to other means of transport shows they are “more dreaded and have higher potential of risk for dying” (p. 20-21). As there have been some higher profile insider incidents involving crew in the past, e.g. the Metrojet crash (Matthews, 2016), the majority of the flying public will be aware of the fact that crew members may pose a threat to their security. The U.S. Federal Aviation Administration found in 1997 that “the flying public placed more trust in the individuals who affects the safety of flying (pilots, control-lers, maintenance workers) than the public and private institutions that provide and ensure safety” (Ray, 1999, p. 4). Further are passengers aboard a plane said to have an implicit trust in their surrounding environment, as they depend on others instead of themselves (Parker, 2006, p. 9). This suggests that there is an underlying trust extended to flight crew by passengers.

Generally, the risk of insider is acknowledged by all stakeholders in the aviation industry. The governmental american institution TSA ranks the insider threat as one of the most important ones the
industry is facing (Siao, 2017). The ICAO views insider vulnerabilities as “a real concern that need[s] to be addressed” (ICAO, 2017). IATA sees insider as a potential threat and wants to raise awareness for it by supporting airlines with background information and ideas for a “risk based approach” (IATA, 2015). Researching the keywords 'insider threat' and 'risk' on the website of ICAO and IATA shows that the insider is one of many risks. The examined airline's view on the insider threat coincides herewith. Crew members are not especially accentuated in the group of insider. Due to their proximity to the aircraft, they are nevertheless perceived to be part of the highest risk group.

In the case study the issue of risk mitigating measures entailing further background checks and continuous evaluations of employees was breached. For many airlines this will be difficult to realize due to laws and regulations in their countries. These mitigating measures may infringe with a person's right to privacy and create an environment similar to a surveillance society. This would also cause an outcry by the public, particularly in western countries. Depending on the course of events of an insider attack, a political mobilisation is imaginable. Through an extensive media coverage on an incident, politicians may be pressured into taking action.

7.3 Characterisation and Evaluation

Data on the risk of an insider threat is only retrievable to some extent. The quantity of such incidents remains unpublished as well as reports detailing specifics of the course of events. Further is a clear cause-effect relationship not identifiable. The assessed risk can hence be characterized as uncertain (IRGC, 2005, p. 16; IRGC, 2006, p. 30).

There are possibilities to reduce this uncertain risk. The studied air carrier for example, has implemented a stricter hiring process (Appendix, Interview, p. 95-96). Despite such mitigating measures the risk itself will most likely continue to exist. Could the solution to the problem thus be the substitution of crew? Technical advances make it possible that planes can be flown by computers. The cockpit crew could therefor be substituted by technology. This would however not necessarily depict a less risky scenario, as technical systems can be infiltrated and manipulated. A similar situation presents itself when viewing the cabin crew. Their duties could be executed by machines such as automated galleys and advanced door operating systems. For these technological systems to function an airline requires maintenance staff. They may turn into insider as well and with their access to these systems they again have the ability to cause severe harm. A substitution of human crew members through technology would thus not be more risk adverse but create a similarly risky situation. The threat would simply shift to hacking the airlines computer systems.

Continuing to take the risk has primarily economic benefits for airlines. Without needed
changes, they do not need to invest money in mitigating measures. A continuation of the current status quo also presents risks for airlines. If an insider incident occurs, they will need to explain their previous inaction. Negative publicity is bound to be a consequence and may result in monetary and status loss. Similarly, will government agency's have to account for their lack of earlier intervention through legislation.

People are increasingly relying on commercial aviation when travelling. Statistics have proven that the industry has become safer over the years with fewer accidents occurring today (IATA, 2017). Society hence generally accepts risks connected to aviation. Insider incidents, such as the 2015 crash of Metrojet flight 9268 (Matthews, 2016) have not caused a setback in passenger numbers to the industry (IATA, 2017). Furthermore, do passengers mostly trust their attending flight crew. The findings of the case study suggest that airlines also tolerate the risk of crew turning into insider. Conclusively should the risk of crew members of commercial airlines as insider be evaluated as a tolerable risk. This entails that the risk is pursued, due to its benefits, with risk mitigating measures being installed (IRGC, 2005, p.12).

7.4 Management

Uncertain risks are “managed using 'precaution-based' and 'resilience-focussed' strategies” (IRGC, 2006, p. 15). Choices for these measures require responsible decision makers. Due to the industry's global alignment an international approach to the issue is necessary. The need for action has been acknowledged by institutions such as IATA and ICAO (IATA, 2015; ICAO, 2017). It is the ICAO who establishes policies for international air travel (ICAO, n.d.b). Therefor it should be the UN agency proposing measures in form of policies. National governments of course need to implement these policies and should autonomously provide their nation's airlines with a legal framework that creates a secure aviation environment. Air carriers also bare a responsibility to ensure a secure execution of their flights. They have the possibility to go beyond policies to implement measures mitigating the insider threat. Examples from the studied airline are the inclusion of integrity tests in the hiring process (Appendix, Interview, p. 95) and trainings to raise awareness for the issue (Appendix, Conversation, p. 84). A further measure could be the so called 'four-eye-rule'. Especially american carriers have installed this rule to assure there are always two people present in the cockpit. If one pilot steps out, a flight attendant needs to be on the flight deck for the time of the pilot's absence. EASA recommended for this rule to be implemented with european airlines after the Germanwings accident. Fears that the presence of a flight attendant in the cockpit can create a new risk were ushered
by the European aviation community though. As cabin crew has no operational knowledge over the cockpit, their presence there “will neither improve security nor safety” (ECA, 2016). Further are the background checks often far less extensive for cabin than for cockpit crew. With emergency equipment in the cockpit and knowledge on flying planes publicly available on the internet the security threat is increased instead of reduced (ECA, 2016).

7.5 Communication

By communicating stakeholders and society will understand the risk. Furthermore, it enables them to retrace the decision making process leading to the decided on management (IRGC, 2005, p. 14). As civil society is the most anxious stakeholder, the information they receive should be corroborative in the industry's efforts in reducing the risk of the insider threat. The information given to the public should be condensed and restricted to decided on measures. Presenting them with ready made plans will reassure them of their security. A continuous communication on the risk is also important for the other stakeholders. Here an information flow is vital from the beginning on. This communication can be done via newsletters issued by agencies such as ICAO or IATA or during conferences and meetings of airlines and representatives. Through lobby work airlines can also convey their interests to governments and other respective parties.

7.6 Analysis

To assess the IRGC risk governance framework's applicability to the risk of the insider threat the following concepts were introductory decided upon: Insider Threat, Classification, Process, Acceptable Risk, Tolerable Risk, Intolerable Risk. For a structured approach the composition of the framework will be followed in the analysis followed by concluding remarks.

The first phase of the IRGC's risk assessment is the Pre-Assessment. Therein a frame for the further depiction of the risk, the insider threat to aviation, is decided on and early warning signs are discussed (IRGC, 2005, p. 8). While information on early warnings for the threat are scarce, it was nevertheless possible to re-construct signs of the risk. Reported incidents caused by insider and reports on the phenomenon were interpreted as signs. Based on the literature review and case study it is clear that the concept is known to both academics and the industry. In the reflection of the case study it has been established that the analysed air carrier defined the term insider similarly to
definitions in literature. Their definition will be found in their soon to be published guideline on the insider threat (p. 86). As the industry and the airline frame the insider as a risk, the menace was framed as a risk.

Conducting the second phase of the framework, the Appraisal, proved to be more challenging. This stage demands a fact based risk assessment of scientific measurable factors and an assessment of the stakeholders perception of the risk (IRGC, 2005, p. 10-11). Listing possible effects and damages caused by the risk and their reversibility was possible based on previous documented cases. Here some assumptions were made, as the existent information is limited. A clear cause-effect for the insider threat was not able to be established. This is due to the complexity of the phenomenon and its many influencing factors on it. Impossible was also a calculation of the risk's probability. The lack of information on both the quantity of cases and their course of events leading to the incident made it impossible to conduct the framework in its entirety. Since there have been incidents in the past and academics suggesting such incidents will occur in the future again (Krull, 2016, p. 30), the probability can only be said to be larger than 0%. For this type of risk specifically it may not be necessary to calculate the probability, though. The researched airline suggests that the frequency of past incidents cannot predict the future (Appendix, Conversation, p. 73).

When conducting the concern assessment, the lack of information again proved to be an obstacle. Particularly little on the public’s perception of the insider threat is known. Based on more general attitudes towards aviation deductions were made about the public’s attitude towards the risk. Airlines perception of the risk were based on that of the case study's research carrier. Through public statements and documents found on the internet the remaining stakeholder's perceptions of the risk could be constructed.

In contrast, coming to a conclusion about the risk's characterisation in the third part of the framework, Characterisation and Evaluation, was simpler. Awareness has been raised for the insider threat and various stakeholders have lobbied for, and in some cases initiated, mitigating measures. At the same time passenger numbers in commercial aviation are still rising (IATA, 2017), with insider incidents appearing not to influence this development. Further are airlines still employing flight crew. Characterising the insider threat as a tolerable risk, one that is taken under the premise that risk reducing measures are taken, was hence a straight forward decision. Labelling it an acceptable risk, would have implied that no further measures need to be taken. As the insider threat has become a considerable amount of attention, including the demand for change, this would have been a faulty characterisation. Stating the insider threat is intolerable, on the other hand, would be excessive. It would mean that airlines would eliminate the human component in their flight operations all together.
or discontinue their business. As globally a large percentage of the population increasingly relies on aviation this would not be justifiable.

While the analysed airline does not have the same type of characterisation of risks per definition of the IRGC, they have defined the insider threat as a tolerable risk. They continue to plan flight crew for rotations while simultaneously implementing risk reducing measures. Pre-set by the internal risk guideline they first differentiate risks into distribution, event and qualitative risks (see Chapter 5.2.2) depending on their attributes. The insider threat is attributed a qualitative risk. Within each of the three risk groups a classification is made into an A-, B-, C-, or D-Risk, depending on their impact's significance level and level of indication for their probability. The intersection of the two indicators is converted into the monetary value of the risk's damage. Starting at a D-Risk the classifications are equated in ascending order (Appendix, Guideline, p. 10-11). The airline's risk classifications thus have a different meaning and implication than those of the risk governance framework. Nevertheless, can their risk classification be translated to fit that of the IRGC by examining the company's risk management.

Phases four and five of the framework, Management and Communication, were only briefly discussed. The classification of the risk as tolerable accounts for management measures to be proposed. As the industry has a global character not a single responsible risk manager can be appointed. All industry involved stakeholders bare some responsibility. Measures to mitigate the risk have been proposed and discussed by stakeholders including the analysed airline, who have already implemented some. From the point of view of the airline the most important measure are the initial background checks upon employment (Appendix, Interview p. 96). For existing personnel anew, background checks pose a judicial predicament in many countries (Appendix, Conversation, p. 82). Measures hence need a political and legal backing, which again in a globalised world needs an international cooperation. Going deeper into the risk management would overstep the limitations of a master thesis. Similarly, would an in depth communication strategy require much more research that would exceed this research's limitations.

Recapitulatory it can be said that the IRGC's framework can be applied when assessing the insider threat to commercial aviation. Most questions needing answers to conduct the assessment were answerable. The risk insider threat was operationalizable based on the concepts common aspects in definitions from academics, the industry and the airline. The process of the risk assessment proved to be difficult. The quality of the assessment is heavily reliant on a catholic access to information. As the insider threat has only recently been acknowledged by the aviation industry and explored by academics, information is still fragmentary. Findings from the literature review alone would have not
sufficed for this purpose. Without the case study it would have been impossible to retrace the airline perspective of the risk. Even though the case study helped close many previous information gaps, one crucial piece of knowledge remained to be unknown, the quantity of events. A data base listing insider incidents cannot to be found, thus it is unclear how frequent crew members turn into insider. Calculating the risk's probability was hence impossible. The examined airline notes that the frequency of past incidents cannot predict the future (Appendix Conversation, p. 73). Not the frequency of such events would be interesting but rather the progression of events (Appendix, Interview, p. 94-95). Information hereon would not only help establish a clearer cause-effect relationship it would indicate what type of risk mitigating measures are necessary and where they need to be implemented. Calculating human decision is highly complex and often inaccurate. In combination with the airlines notion that the frequency of the past events cannot predict the future, a question regarding the framework's scientific risk appraisal arises: Is the calculation of a risks probability useful and relevant when the assessed risk is posed by humans?

A lack of research on the public's perception of the insider threat further compromises the accuracy of the assessment. The applications greatest impairment was hence the limitation of accessible data. Nevertheless, was it possible to establish that the public does not perceive the risk to be intolerable. Their perception thus coincides with that of the remaining stakeholder. A classification of the risk could also be made. While the examined air carrier classifies risks not in the same manner as the IRGC, a transferral of the carrier’s risk classification to that of the framework could be done. Based on the appraisal, the risk is rated a tolerable risk.
8. Conclusion

This research's main objective was to find: To what extent can the Risk Governance Framework developed by the International Risk Governance Council be applied to the assessment of the insider threat to commercial aviation?

The term 'insider', relating to aviation, includes a wide variety of aviation employees with diverse possibilities to cause harm. For the purpose of the study the term was hence confined to cabin and cockpit crew of commercial airlines. As research on the insider threat is still in its early stage, a case study on an airline's approach to the risk was conducted. Hereby their risk management and perception of the insider threat was explored. It was found that the company follows a methodical approach to risks that distinguishes them first into categories according to their characteristics and then according to their financial damage. The insider is a recognized risk that is given much attention by the carrier, though it is only one of many risks they are managing. Within the group of insider crew members are not given special attention.

Together with the knowledge gained from the literature review the IRGC's framework was applied to the insider threat. Due to the risks unseizable character it is an uncertain risk that, nevertheless, is found to be tolerable.

While an assessment of the risk was possible to be made, the framework, at times, proved to be difficult to apply. It demands a thorough literature review and access to data. As the assessed risk is a security sensitive matter, publicly accessible data is scarce. Therefore, parts of the framework could not be applied. Especially the risk’s appraisal could not be conducted in its entirety. Particularly the scientific risk assessment fell short of its calculation of the insider threat's probability. It is not clear whether more accessible data would have changed the result of the risk assessment.

The examined airline's risk perception of the insider threat was assumed to be that of all airlines during the risk assessment. This assumption may not be correct due to cultural differences or experiences that other air carriers have made. Further was the term 'insider' limited to one fragment of insider. The risk assessment of other types of insider may be different to that of crew and may also pose different challenges for the framework's applicability. Generally, it is found that the IRGC's framework is reliant on comprehensive information. When assessing security related risks this information is not always accessible. This tarnishes the framework's applicability. The question of the framework's necessity and usefulness for calculating the probability of a risk posed by humans,
was raised. Research hereon would be a contribution to the IRGC's work and to that of security risk studies. With further research into the insider threat a more extensive literature review will be build. This presents the possibility to conduct the framework in its entity and re-evaluate the research guiding question.
Bibliography


