FFI-RAPPORT

16/00707

A risk assessment of the Piql Preservation Services

future preservation – future risk

–

Ulrikke Agerup
Kjell Olav Nystuen
Janita Bruvoll
Kjersti Brattekås
Monica Endregard

A risk assessment of the Piql Preservation Services

future preservation – future risk

Ulrikke Agerup
Kjell Olav Nystuen
Janita Bruvoll
Kjersti Brattekås
Monica Endregard

Norwegian Defence Research Establishment (FFI) 24 June 2016

Keywords

Risikovurdering
Scenarioer
Morfologisk analyse
Datalagre
Langtidslagring

FFI-rapport

FFI-RAPPORT 16/00707

Project number

511501

ISBN

P: 978-82-464-2766-9
E: 978-82-464-2767-6

Approved by

Kjersti Brattekås, *Research Manager*
Janet M. Blatny, *Director*

Summary

This report is the Norwegian Defence Research Establishment (FFI) deliverable in work package (WP) 1 “Mapping of technologies and regulations” of the project “Preservation: Immune and Authentic” (PreservIA), supported by the Research Council of Norway (RCN). The aim of the PreservIA project is to improve a newly developed technology for long-term preservation of digital data (the Piql Preservation Services) to better ensure the security, immunity and authenticity of the information stored on the storage medium, the piqlFilm. The application of the service is both universal and global, and the components of the service have a life span of 500 years or more.

The aim of the risk assessment is to identify the vulnerabilities of and challenges to the service. It was assessed by how well it could maintain the confidentiality, integrity and availability of the information, which are key properties of information security. The assessment uses the scenario-based approach, and the morphological method of scenario development was used to arrive at a set of scenarios covering the risks to the service used in the scenario analysis.

Due to the scope of the assessment –a result of the wide application of the service and a long time perspective – simplifications were necessary in order to create suitable scenario descriptions. The scenario classes used were accident, technical error, natural disaster, crime, sabotage, espionage, terrorism, armed conflict and nuclear war. As this is a large number of scenario classes, and as it was necessary to include an even larger number of scenario descriptions, we used a scenario template for this purpose. The final scenario analysis identified several vulnerabilities. Some were severe, such as fire, chemical compounds and the inside threat from theft and sabotage. Some were less severe, such as the effect of electromagnetic pulses and nuclear radiation. Some simply require more testing before FFI can say anything definitive about the effects and consequences for the information stored with the Piql Preservation Services, such as the effects of water, smoke and pressure from overhead weight.

The main weakness of the Piql Preservation Services was found to be the vulnerability of the emulsion layer on the piqlFilm, upon which the digital information is written. Robust protective measures surround the service, but the inside threat is still serious, as is sabotage due to the many components which can be affected. Strengths include plastic as the choice of material, automated storage as the storage management method, and relatively strong computer security mechanisms, including the piqlFilm being effectively offline. FFI has made several recommendations to mitigate these risks, which may be implemented in later work packages when requirement and design specifications are revised and new prototypes are developed. FFI will then have an advisory role and be available for discussions on implementations.

Sammendrag

Denne rapporten er FFIs leveranse i arbeidspakke (AP) 1 “Mapping of technologies and regulations” i Norges forskningsråd-prosjektet “Preservation: Immune and Authentic” (PreservIA) 2015-2018. Formålet med PreservIA-prosjektet er å forbedre en nyutviklet teknologi for langtidslagring av digital data (the Piql Preservation Services) slik at sikkerheten, immuniteten og autentisiteten til informasjonen som blir lagret, blir bedre ivaretatt. Anvendelsen av tjenesten er både universal og global, og de ulike komponentene som utgjør tjenesten har alle en levetid på 500 år eller mer.

Hensikten med risikovurderingen er å identifisere sårbarheter og sikkerhetsutfordringer ved tjenesten. Systemet ble vurdert ut fra hvor godt det ivaretok konfidensialiteten, integriteten og tilgjengeligheten til informasjonen som blir lagret, som er grunnleggende egenskaper ved informasjonssikkerhet. Risikovurderingen har en scenariobasert tilnærming, og morfologisk metode for scenarioutvikling ble brukt til å komme frem til et sett med scenarioer som dekker risikoene tjenesten står overfor. Disse scenariobeskrivelsene ble brukt i scenarioanalysen.

Med tanke på vurderingens omfang, grunnet tjenestens brede anvendelse og det lange tidsperspektivet, var det nødvendig å gjøre visse forenklinger for å danne passende scenariobeskrivelser. Scenarioklassene som ble brukt var ulykke, teknisk feil, naturkatastrofe, kriminalitet, sabotasje, spionasje, terrorisme, væpnet konflikt og atomkrig. Fordi dette er et stort antall scenarioklasser, og også fordi analysen gjorde det nødvendig å inkludere enda flere scenariobeskrivelser, måtte vi bruke en scenariomal til dette formålet. Den endelige scenarioanalysen identifiserte flere sårbarheter. Noen var alvorlige, som effektene av brann, kjemiske stoffer og innsidetrusselen for tyveri og sabotasje. Andre var mindre alvorlige, som effekten av elektromagnetiske pulser og radioaktivitet. Andre igjen, som effektene av vann, røyk eller trykk, krever mer testing før FFI kan konkludere når det gjelder effekter på – og konsekvenser for – informasjonen som lagres med the Piql Preservation Services.

Den største svakheten ved the Piql Preservation Services ble vurdert til å være sårbarheten til emulsjonslaget på lagringsmediet – piqlFilm – der informasjonen er skrevet. Gode sikkerhetstiltak finnes rundt tjenesten, men innsidetrusselen er fremdeles en alvorlig. Det samme kan sies om sabotasje, da det er flere sårbare komponenter i systemet som kan angripes. Styrker ved tjenesten inkluderer valget av plast som hovedmateriale, automatisk lagring som lagringsmetode og relativt gode informasjonssikkerhetsmekanismer, inkludert at lagringsmediet stort sett er offline. FFI har flere anbefalinger til hvordan disse truslene kan modereres. Anbefalingene kan implementeres i senere arbeidspakker når krav- og designspesifikasjoner skal endres og nye prototyper utvikles. I disse arbeidspakkene vil FFI ha en rådgivende rolle og vil være tilgjengelig for diskusjoner vedrørende implementeringene.

Content

List of Tables

List of Figures

Preface

The authors would like to extend their thanks to FFI researchers Agnieszka Anna Gorzkowska-Sobas, Berit Harstad Gilljam, Halvor Kippe and Odd Harry Arnesen for valuable insights on different subjects related to this assessment, and special thanks to FFI researcher Odd Busmundrud for calculating heat dissipation.

Special thanks to the Norwegian National Archive for making time to give an instructive introduction to archival procedures, for highlighting the needs and concerns one must pay special attention to when dealing with long-term preservation, and for sharing their concerns and wishes regarding safety and security.

Finally, this report would not have been possible had it not been for fruitful discussions and important documents made available by the PreservIA project Consortium partners.

Ulrikke Agerup

Kjeller, 24.06.2016

1 Introduction

It was Aristotle who said “It is likely that unlikely things should happen” [1 p.357]. In other words, we must accept the probability of the improbable occurring, because only when we accept it can we begin to plan for it. That is the purpose of risk assessment: to identify and evaluate the risks surrounding us to be able to mitigate the effects of those risks. It is true of all risk assessments and future studies that the unknown and the uncertainty of what the future might bring is a defining factor, but in the risk assessment presented in this report this aspect is multiplied a hundredfold. It will make an assessment of the risks faced in long-term preservation of digital data for 500 years to come. Considering the exponential change rate our society is experiencing, it is simply impossible to predict from a scientific point of view what our world and our reality will look like in 500 years from now and hence the risks we then have to face. Additionally, we have to take into account the limitations of human perception and imagination, where we are unable to even imagine, and thus foresee, events which may occur. This state of non-imagination is magnified in our assessment because of the vast time perspective. Artificial intelligence, dinosaurs roaming the earth once more due to genetic manipulation of frozen DNA, the extermination of the human race due to plague, meteor showers, and many other events which lie outside the scope of our imagination – these are all events which may happen within the next 500 years, and if they do, they could to great harm to the Piql Preservation Services, the object of study in this report. However, though it is important to allow room for such fantastical thinking in the assessment, as this is a scientific report we must mainly deal with trends and events we can perceive.

In this study FFI is performing a risk assessment of the Piql Preservation Services, which represents a new and innovative solution to long-term preservation of digital data. As an alternative to the traditional storage media – hard disks, optical disks and magnetic tapes – the information is stored instead on a proven technology for audio-visual preservation – photosensitive film. This film is taken in use within the Piql Preservation Services as a newly developed “nanofilm”, with the same proven properties as the more traditional microfilm. This new film, the piqlFilm, has a documented longevity of at least 500 years, eliminating the need for data migration. The report is a deliverable in one of many Research & Development projects Piql AS is currently running simultaneously in order to continuously improve the technical quality of the components of the Piql system, as well as advance its security properties. The project is called “Preservation: Immune and Authentic” (PreservIA), and its goal is to further develop future versions of key components of the Piql system to improve functionality and thus better ensure the security, immunity and authenticity of the information stored on the piqlFilm.

The risk assessment in this study entails identifying vulnerabilities and security challenges the Piql Preservation Services may face now and in the next 500 years throughout the Piql Preservation Services Journey. Which steps this service journey include and how the scope of the assessment is defined, is clarified in chapter 2 and 3 of the report. The vulnerabilities and security challenges identified will be analysed according to their effect on the three main security properties of information security: confidentiality, integrity and availability. The purpose of the study is to assist the development of a product for the targeted application areas which in a security context is adapted to the market’s needs. That is why FFI’s perspective while assessing the risk towards the Piql Preservation Services is user-oriented.

To solve the task outlined above, we have chosen a scenario-based approach. FFI has much experience with this method, and it is suitable to the assignment. Due to the large intended application area of the Piql Preservation Services, we need a structured way of identifying its weaknesses and security challenges. Morphological analysis is a method to structure and analyse complex problems, making it the perfect tool to assist us in making a suitable selection of scenarios. The scope of the project further indicates that a large number of scenarios is needed to make sure the risk assessment covers all the relevant hazards and threats facing the Piql Preservation Services. Describing in full detail such a large number of scenarios lies outside the scope of this assignment. Consequently, we have developed a scenario template which enables us to include a greater number of scenarios in the assessment without the risk of omitting important details. Based on the vulnerabilities and security challenges identified for different application areas in the scenario analysis, we outline development tasks and changes that could be made to the design and requirement specifications of the Piql System which should help to solve these security issues.

Additionally, the report includes a brief overview of alternative digital storage technologies which are available on the market today – e.g. hard disks (HDD), optical disks (CD) and magnetic tapes (LTO) – in order to place the Piql Preservation Services in a wider context. After their general features are introduced, their security qualities are briefly discussed. It will become evident that the Piql Preservation Services possess some qualities which make it better suited for long-term preservation, both with regards to functionality and for security purposes.

1.1 Document Structure

This report is structured in 11 chapters. Chapter 2 serves as a background chapter and gives a brief introduction to the Piql Preservation Services, in order to give the reader an understanding of the service which is sufficient to follow our assessment of the risks which may threaten it. During this introduction the scale and complexity of the Piql Preservation Services will become clear: for now it is sufficient to note that Piql AS’ vision for the system is both universal and global in its application, and the longevity of the components storing the information is 500 years. It is necessary, then, in chapter 3 to clarify and specify the scope of the assessment. It is equally important to define the key terms which are used throughout the report, which is done in chapter 4.

Chapter 5 outlines and explains the simplifications and specifications we found necessary to clarify while developing the appropriate scenarios for the scenario analysis. There proved to be so many elements which needed to be considered because the scenarios have to cover a service this size, that we were required to make certain standardised assumptions about the present and future application of the Piql Preservation Services. These we outline as various categories, often consisting of different sub-categories.

Chapter 6 first explains why we have chosen the scenario-based approach to do this risk assessment, and briefly summarises the considerations which must be taken into account in the scenario analysis in order for the risk assessment to be considered complete. It goes on to presents the method we have chosen in the report to make a relevant selection of scenarios: morphological analysis. First the technical aspects of the method are explained, and then it is applied to issues of safety and security separately. Finally, the final selection of scenarios for further analysis is presented.

We have created a template to use for the scenario descriptions, as there were so many of them. Chapter 7 explains further why such a template is useful and how it is meant to be used. Including all of the completed templates in the report would be too extensive. Hence, chapter 8 only briefly depicts the contents of the various scenarios, whereas the full details of the completed descriptions are included as appendixes to the report. The vulnerabilities and security challenges of the Piql Preservation Services which are identified in the scenario analysis are presented and discussed in chapter 9, followed by the comparative overview of the different digital storage media available for long-term preservation in chapter 10. Chapter 11 builds on the analysis in chapter 9 and discusses the relevant recommendations to be made to alleviate these issues. Finally, chapter 12 concludes the report.

2 The Piql Preservation Services

Before risks can be identified, we must first describe and examine the object of study – the Piql Preservation Services – in order to understand the system and, in turn, locate critical points of vulnerability. In the following we will therefore give an introduction to the Piql Preservation Services. The purpose of this introduction is not to give an in-depth description of the system and all its features and innovations. What we are aiming to do is give the reader an understanding of the Piql Preservation Services which is sufficient to follow our assessment of the risks which may threaten it.

The Piql Preservation Services is a complete system for long-term preservation of digital data [2]. Piql AS has, through several R&D projects in collaboration with various Consortium partners, developed the technology and the different components needed to preserve digital data for a timespan of over 500 years in such a way that ensures the data’s authenticity, immunity and security.

The system includes hardware for writing and reading data on the storage medium, *piqlFilm*, which is placed in a primary packaging, *piqlBox,* to protect the PiqlFilm against its external environment. The piqlBox is in turn placed in a secondary packaging, *piqlBin*, which is suitable for handling in a fully automated storage system, called a *piqlVault*. The process is connected to a web-based system for data ingest and retrieval [2].

The piqlFilm is a new type of photosensitive film. It consists of a base material made of polyethylene terephthalate (PET) and a gelatine emulsion containing photo-active chemicals such as silver halide crystals as coating. This unique coating will increase the data density on the film, while preserving its longevity, making it possible to replace e.g. five hundred boxes of paper with a single reel of piqlFilm.

The piqlBox is made of polypropylene (PP). The materials used were selected because they do no harm to the piqlFilm or its longevity in any way, while at the same time guaranteeing over 500 years longevity for the piqlBox itself.

The piqlBin is a component of the piqlVault, which uses the automated AutoStore® system as its storage system. The AutoStore® system is a unique Automated Storage and Retrieval System (AS/RS), operated by multiple robots picking up the piqlBins from a specially designed grid and transporting them to an operator port for retrieval by a human operator. The qualities and features of the modified AutoStore® system used in the Piql Preservation Services and the specific storage conditions under which the piqlFilm and –Box will be stored will be elaborated upon in chapters 3 and 5.4 of this report.

In order to gain a proper appreciation for how the Piql Preservation Services works, it is useful to go through the service journey or the service workflow step by step to understand how analogue data ends up on a piqlFilm in a secured storage facility [3, 4]. This journey is depicted in figure 2.1. First, though, it is necessary to understand Piql AS's vision for the application of the Piql Preservation Services. The system is delivered as a service to the market through selected Piql partners. These partners shall function as hubs of activity across the globe, where one such partner is responsible for delivering the service to multiple end users, i.e. data owners in need of archival and preservation services across sectors and industries. Piql AS' vision for the application is, in other words, both global and universal.

The service journey starts when born digital data or digitised data is sent to a Piql partner by a data owner. When the data is received, integrity checks are performed to make sure that, firstly, none of the information was altered during the reception of the data, and, secondly, that no viruses or other malware are transferred into the Piql system. The original data is then ingested into the computer system where a data preparation process is automatically started. This process serves two main purposes: to collect and store relevant metadata to enable future access to the data; and to encode the data and metadata into the Piql system storage format, comprising a single file.

Here the data owner has a choice between different ways to preserve the data: a digital, visual or hybrid preservation of the data. The digital option encodes all the data into binary form, which is not understandable to the human eye. The visual option maintains readability, where the data is printed as text or pictures. Lastly, the hybrid option is a cross between the two former, where some of the data is encoded into binary form and some is printed as text or pictures. The computer prepares the data according to the option chosen by the data owner. The original data is also, for the time being, kept in the Piql computer system.

Now, the data writing process can begin. Using a closed internal network, the prepared data is sent to the piqlWriter, an especially developed high resolution writer of the piqlFilm. After an additional integrity check, the file is ready to be written. Loading the piqlWriter with the piqlFilm and preparing the writing process must be done manually by a Piql Preservation Services operator, one which does not have the necessary access to the computer and thus the original file. Once the piqlFilm is written it is sent to a separate location to be developed or processed using a special mix of chemicals adapted to the qualities of the film. It is then sent back to the production site where it is fed into a piqlReader, a high resolution film scanner, which reads back all the data on the piqlFilm to verify its contents frame by frame against a checksum created when the original files were received from the data owner. Only when the piqlReader verifies the integrity of the newly written piqlFilm is the original file of the data deleted from the computer system. The finished piqlFilm is then assembled and packed in the protective piqlBox and finally, if the data owner has chosen to store the data with a Piql partner, it is transported to a secured automated offline storage facility.

Metadata from each individual piqlFilm is stored in an online database. The data owner can use this to search for a specific file within a piqlFilm and request its retrieval from the piqlVault. After the file on the piqlFilm is read back on a piqlReader and its identity and integrity is confirmed, the file can be delivered to the data owner either electronically or by a physical storage medium (e.g. hard drive). To read the piqlFilm reel in its physical form, in theory, all one needs is a light source and magnifying lens, if the preservation method is visual. If the data is preserved with the digital method, one would also need a camera and a computer. Each film begins with a series of frames which contains information in human readable format on how the data stored on the film can be read or retrieved. If the data is discernible to the naked eye, i.e. in the format of text or pictures, it can be read immediately. If the data is encoded into binary form, the first frames will outline instructions on how to decode the frames back to files. In this way, the information on the piqlFilm is self-contained, or without need of non-accessible equipment or software to read it back.

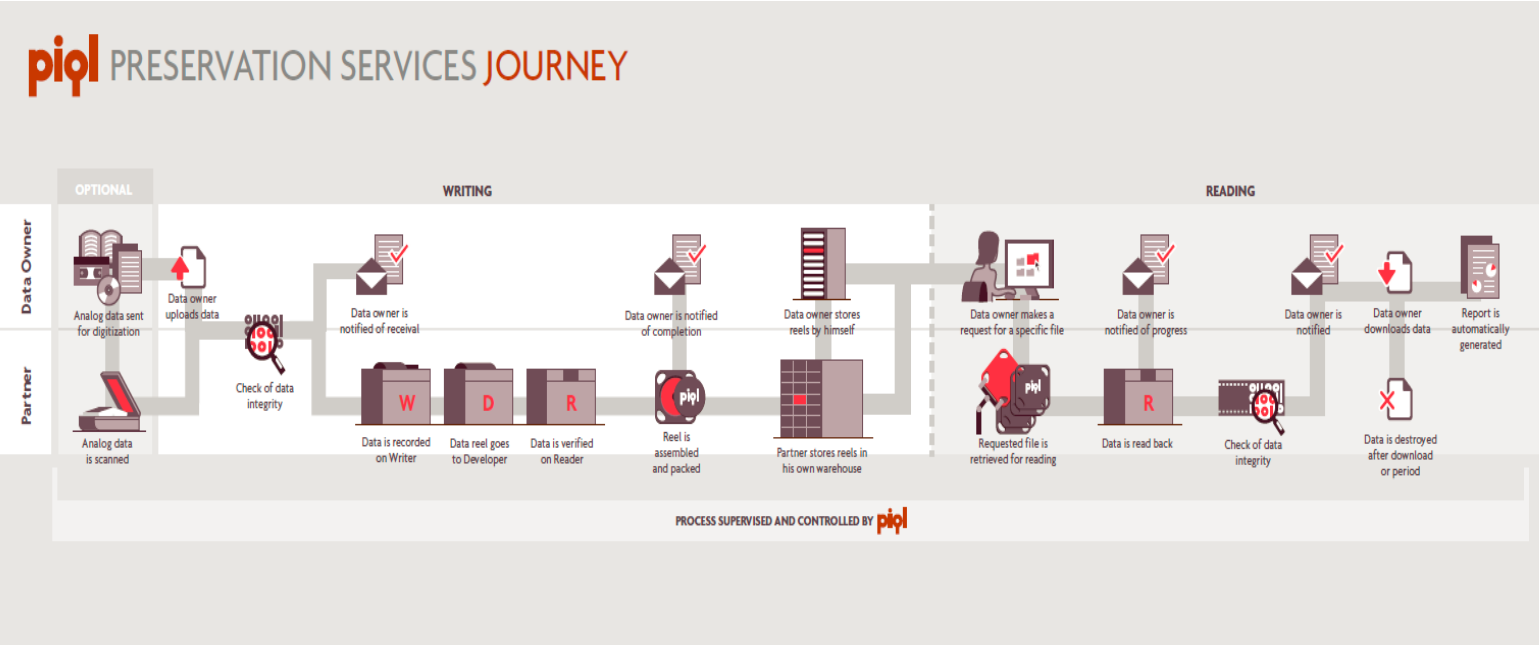

piql PRESERVATION SERVICES JOURNEY
OPTIONAL
WRITING
READING
Data Owner
Partner
Analog data sent for digitization
Analog data is scanned
Data owner uploads data
Check of data integrity
Data owner is notified of receival
Data is recorded on Writer
W
Data reel goes to Developer
D
Data is verified on Reader
R
Data owner is notified of completion
Reel is assembled and packed
piql
Data owner stores reels by himself
Partner stores reels in his own warehouse
Data owner makes a request for a specific file
Requested file is retrieved for reading
Data owner is notified of progress
Data is read back
R
Check of data integrity
Data owner is notified
Data owner downloads data
Data is destroyed after download or period
Report is automatically generated
PROCESS SUPERVISED AND CONTROLLED BY piql

Figure 2.1 The Piql Preservation Services Journey. Source: Piql AS

3 Scope

The Piql Preservation Services is a complex system, with several components with various features, and both a production and a storage phase. When we recall that Piql AS' vision for the system is both universal and global, and we add to that a time perspective of 500 years, we begin to comprehend the complexity of the Piql Preservation Services and thus the intricacy of doing a risk assessment of this system. Because of this complexity it is necessary to limit the field of our risk assessment. First, however, it is pertinent to outline what is meant by risk assessment. Yet, before explaining our approach to doing a risk assessment, we must clarify some term usage. In this report, we are using the term *risk assessment*, not threat assessment or threat analysis. The term risk covers both intentional acts and unintentional events and does not therefore risk excluding the latter, as the term threat can do. Additionally, according to the definition we follow here, an analysis is only a small part of an assessment, and we aim to evaluate more than would be covered by an analysis.

Risk assessments, be it for a product or a business model, are a method to better manage risks. Knowing which threats or hazards may harm our objectives and which vulnerabilities our values have can allow security measures to be put in place, which lets us control the risk and determine it at a level which is found acceptable and tolerable. By including a risk assessment as part of a R&D project, Piql AS ensures that risks are identified early in the development process of the system, so that new or modified design and manufacturing requirements for version two of the piqlFilm and -Box can be implemented. Moreover, security parameters surrounding the piqlVault can also be recommended to the end users.

Different approaches to risk assessment and how best to apply them in real life is a contested issue in the field of societal security and preparedness. There are two main approaches used in Norway:[1] the NS 5814, which is based on SN-ISO Guide 73:2009 [5], and the newer NS 5832 [6]. They are in part competing approaches, and there is a lot of discussion in different work and research environments as to which is the better one to use. FFI has also been instrumental in this discussion, recently completing a thorough study on the subject specifically on the merit of the different approaches when it comes to preparing for unwanted intentional acts [7]. Their conclusion is, not surprisingly, that both approaches have their strengths and weaknesses, and that they can – and perhaps should – complement each other for a better result.

We will use the more scientifically founded terminology of the NS 5814 as the general framework for our risk assessment approach. Within this framework, however, we incorporate the three factor model presented in the NS 5832 into the analysis, which captures the relationship between value, threat and vulnerability. This value-oriented thinking is essential to this risk assessment. In order to develop a product for the targeted application areas which in a security context is adapted to the market's needs, we need to start by gaining an understanding of which assets each application area needs protected, i.e. what type of information and the

[1] Norway is used as a frame of reference, as this is where we have the most experience. The standards used are also representative of other national standards.

corresponding sensitivity of that information. This could vary greatly from area to area: military secrets are a lot more sensitive, for instance, than a company's accounting records. The security level surrounding the Piql Preservation Services would vary in equal measure. Before we can make sound recommendations regarding the security level needed to protect the asset, we must first understand the value of the asset in order to analyse what kind of threats it faces and thus what its vulnerabilities are. The value-oriented thinking is therefore paramount to our risk assessment.

Based on the discussion above, we present our working definition of a risk assessment. A risk assessment is the overall process of risk identification, risk analysis and risk evaluation. By risk identification we mean first mapping the system which is the object of analysis, here the Piql Preservation Services, followed by finding and describing corresponding risks. The next step, risk analysis, entails assessing the relationship between the intentional threats or unintentional hazards faced by a certain value and the vulnerability of this value against the specified threat or hazard. Lastly, risk evaluation involves determining the level of risk and identifying corresponding measures to reduce the harmful effect [5, 8]. Our emphasis in the PreservIA project is primarily placed on the first two, whereas the risk evaluation will serve to form the basis of further work in later work packages in the PreservIA project.

As stated in chapter 1 of the report, our risk assessment will cover the Piql Preservation Service Journey. However, a more in-depth clarification of the scope is necessary, firstly, because we include considerations which go beyond the service journey as explained in detail in chapter 2, and, secondly, because certain aspects of - and stages in – the service journey are not covered by our assessment.

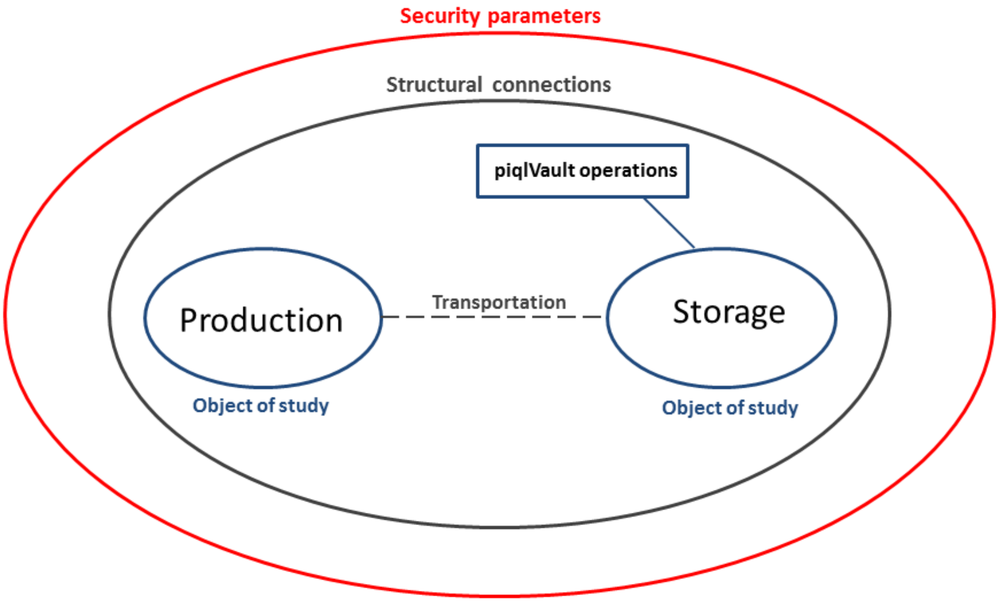


Figure 3.1 The scope of the risk assessment

A concise and schematic overview of which processes – or objects of study – the risk assessment in this report will include is depicted in figure 3.1 and 3.2.

Figure 3.1 illustrates the entire scope of our assessment. First, two specific objects of study are depicted: the production phase and the storage phase, shown in blue. These we remember from the service journey. The production phase includes the entire process, from the reception of the digital data until the finished reel is placed in a piqlBox, and the storage phase is while the piqlFilms are in storage. The storage object also includes the operational processes of running the automated storage facility, i.e. the piqlVault, which is elaborated upon below in figure 3.2. Second, the structures surrounding and connecting these objects are depicted in grey. The main structural connection we emphasise is the transportation phase, when the piqlBoxes are transported from the production site to the designated storage facility. This step is also included in the service journey. Finally, encapsulating all the objects and processes are the security parameters surrounding the Piql Preservation Services, which is shown in red. These include the safety requirements of the storage facility and security regime that applies during production, during transportation and while the piqlFilms are in storage. Identifying the vulnerabilities and security challenges which exist within this scheme is the purpose of this report and forms the basis of our assessment.

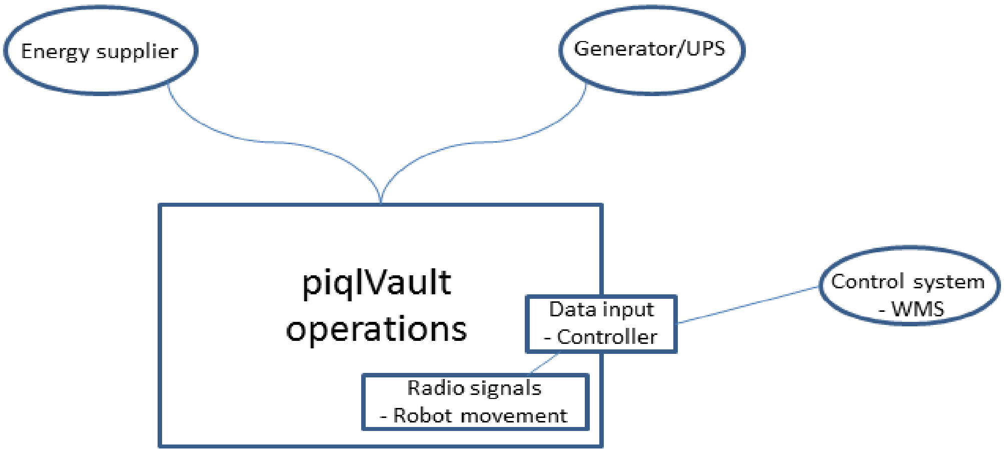


Figure 3.2 The piqlVault operations

Figure 3.2 illustrates visually how the automatic operating system in the storage facility is set up [9]. A more thorough and detailed description of the automated storage system is given in chapter 5.4. Here, we simply outline the critical external structural dependencies of the modified version of the AutoStore® system which is used in the piqlVault to give the reader an understanding of the elements we focus on in the risk assessment.

The AutoStore® system has two direct external connections into the system: One is the electric power supply. The AutoStore® is fully automated, which means it is fully dependent on the supply of electricity to operate. In case of a power outage or loss of utilities, the AutoStore® system is equipped with one generator which supplies additional electricity for 24 hours.[2] This is to make sure the system has enough electricity to shut down properly and avoid related complications. The other external connection is the interface network between the internal closed network of the AutoStore® and the external network of the Piql partner. Through this interface network the AutoStore® receives data input from the Warehouse Management System (WMS) through the AutoStore® Controller, which in turn sends radio signals giving the robots instructions on the handling of the piqlBins holding the piqlFilms.

First, it must be made clear that we will only look at the production process which entails the printing of data on the piqlFilms, and not the production process of raw materials for the components themselves, i.e. the empty piqlFilm and piqlBox, prior to the printing process. Each supplier of the Piql components will perform individual “Failure mode and effects analyses” (FMEAs), outlining where in their production chain a failure may occur and the effects thereof. Similarly, problems which may occur while a Piql partner is writing the finished piqlFilms for a user, such as faulty equipment or human errors, which may have a negative effect on the piqlFilms, fall outside the scope of our assessment. This is part of Piql AS’ internal assessment of the production process, whereas we will mainly include external risks to the production process.

Secondly, in the scenarios relating to storage, our assessment is limited to storage in piqlVaults, i.e. storage facilities owned and operated by Piql partners. Each data owner has the option of storing their piqlFilms in a private storage facility, but these will not be covered by this assessment. Nevertheless, the findings and recommendations in the report may serve as guidelines regarding the security measures put in place in such private storage facilities.

Lastly, this report will not include the final step in the service journey: that of data retrieval. We have not placed much emphasis on the online-based processes of the Piql Preservation Services, as the vulnerabilities and challenges present here are common to all digital storage mediums which depend by their very nature on online access. Therefore, we will instead focus our attention on the production process and the offline storage of the medium, as these are unique to the Piql system.

However, a risk assessment of the Piql Preservation Services cannot be complete without the inclusion of challenges related to data security. In order to fully evaluate security, one must understand the interaction between the physical and the digital properties of a system.[3] As a service for the preservation of *digital* data, the Piql Preservation Services is intrinsically linked to the online realm, and threats to data security thus cannot be excluded from the assessment, as we include therein more phases of the service journey that merely storage. One should, however, stress that the actual *storage medium* – the piqlFilm – is offline, referring to the fact

[2] The assumption regarding the longevity of the generator’s power supply was made in collaboration with Piql AS.

[3] This was a key conclusion in the FFI report “*ICT and CBR related threats against Oslo Water and Sewage Authority*” [freely translated] [10].

that while the piqlFilms are in storage, they have no connection to online networks. Yet, in order for the piqlFilms to become just that – a film with printed information on it as a vital component of the Piql Preservation Services – the piqlFilms must at some point be connected to online networks, for instance when they are placed on the piqlWriter- and Reader. These processes are necessary both during data ingestion and data retrieval, and risks and vulnerabilities connected to data security are present in both these phases. Because of the similarity of threats, we therefore include only the ingestion phase in our risk assessment, as we deem it unnecessary to include both.

4 Definitions

This chapter provides working definitions of key terms utilised in this report and specifies important delimitations. The subjects touched upon requiring clarifications are risk and vulnerability analysis, computer security and the scenario-based approach.

4.1 Terms Related to Risk and Vulnerability Analysis

Term	Definition
Safety	Protection against unwanted events that are caused by one or more coincidences, i.e. unintentional events [11, 12].
Security	Protection against unwanted events that are the result of deliberation and planning, i.e. intentional acts [11, 12].
Risk	Expression of danger of loss of important values due to an unwanted event. SN ISO Guide 73:2009 defines risk as the effect of uncertainty on objectives, often expressed in terms of a combination of the consequences of an event and the associated likelihood of occurrence. NS 5830:2012 defines risk as the expression of the relationship between the threat against a given asset and this assets vulnerability to the specific threat [11, 5 p.3, 13 p.5].
Threat	A possible unwanted event that can have negative consequences for the security of an entity [13 p.4]. Used in this report in relation to an action performed by a threat actor, i.e. an intentional act.
Hazard	Source of potential harm [5 p.7]. Used in this report in relation to an event without a deliberate cause, i.e. an unintentional event.
Vulnerability	ISO Guide 73:2009 defines vulnerability as the intrinsic properties of something resulting in susceptibility to a risk source (element which alone or in combination has

	the intrinsic potential to give rise to risk) that can lead to an event with a consequence. NS 5830:2012 defines vulnerability as lack of ability to withstand an unwanted event or maintain a new stable state if an asset is subject to unwanted influence [5 p.8, 13 p.5].
Risk assessment	Used here as a working definition: Overall process of risk identification (process of finding, recognising and describing risk), risk analysis (process to assess the relationship between the intentional threats or unintentional hazards faced by a certain value and the vulnerability of this value against the specified threat or hazard) and risk evaluation (process of determining the level of risk and identifying corresponding measures to reduce the harmful effect).[4]

Table 4.1 Terms related to risk and vulnerability analysis

4.2 Terms Related to Computer Security

Term	Definition
Information security	Pre-emptive measures to secure the confidentiality, integrity and availability (CIA) of sensitive information throughout its existence. It is common to include measures to secure authenticity as well [11, 14 § 5,1, 15].
Confidentiality	The prevention of unauthorised disclosure of information [16 p.34, 14 § 5,3-b].
Integrity	The prevention of unauthorised modification of information [16 p.35, 17, 14 § 5,3-c]. I.e. the information is preserved unaltered with the information content as it is supposed to be.
Availability	The prevention of unauthorised deletion or removal of information. The property of being accessible and usable upon demand by an authorized entity [14 § 5,3-d, 16 p.36].
Authenticity	That the information is what it portrays itself to be. The property of being real and authentic [17, 14 § 5,1].
Immunity	In the PreservIA project context: Immune against the alteration of CIA.
Data	Physical phenomena chosen by convention to represent certain aspects of our conceptual and real world. The meanings we assign to data are called information. Data is used to transmit and store information [16 p.40].
Information	The (subjective) interpretation of data. Any form of intelligence in material or immaterial form [16 p.40, 18 § 3,7].

[4] Our working definition is a combination of the definitions found in SN-ISO Guide 73:2009, NS 5830:2012 p.5 and Rausland & Utne (2009) p.77.

Term	Definition
Asset	The physical representation of a value. A resource that, if exposed to unwanted influence, will bring about a negative effect for the person who owns, manages or profits from the resource [13 p.4]. Used here as a synonym for the data on the piqlFilm in need of storage and protection.
Value	The assigned worth of an asset.

Table 4.2 Terms related to computer security

4.3 Terms Related to the Scenario-Based Approach

Term	Definition
Scenario development	The process of (i) mapping all the relevant elements to be included in a scenario to ensure the validity of a given assessment and the ability to make meaningful conclusions about the object of analysis, and (ii) ensuring the selection of scenarios suitable to address the problem.
Scenario description	The process of writing out the details of the elements of a given scenario found relevant during the process of scenario development.
Scenario analysis	The process of drawing conclusions based on the findings identified in the scenario descriptions and, in turn, make relevant recommendations.

Table 4.3 Terms related to the scenario-based approach

5 Simplifications and Specifications

Due to the scale of the object of analysis – the Piql Preservation Services, with all three components (film, box and vault) and the complexity of the service journey – it became apparent that a simplification of the subject matter was required to enable an adequate scenario development process which in turn would lead to a meaningful scenario analysis relevant to this study. Accordingly, we were obliged to make certain standardised assumptions about the present and future application of the Piql Preservation Services for the purpose of this assessment.

We have made clearly defined classifications for the categories geography, timeframe and user class, with the corresponding asset in need of storage and protection in that user class. In addition we have, in collaboration with Piql AS, made an operative concept which describes the location and the layout of the storage facilities, as well as accounting for the security surrounding the Piql Preservation Services. This comprises the safety requirements which are in place and the security standards and procedures that apply in and around the storage room. We have formulated methods to implement the set of security standards set forth by Piql AS, which should be in place during the production and transportation phases as well. As security must be evaluated as a whole, we touch upon regimes of both physical and computer security.

By creating a synthetic reality in this way, we are allowed more control over the different elements which have to be included in the scenarios to make them plausible and realistic. Without such simplifications the scenarios would be too comprehensive to allow them to be part of a larger analysis later. As stated, our perspective in this assessment is user-oriented, meaning that the choices we made in the simplification process which follows, and later when describing the scenarios as well, are made with the demands and needs of the user in mind. The simplifications are also a way of making the scenarios more universally applicable. A potential user of the Piql Preservation Services would then more easily be able to apply the more generic scenarios presented in this report to their own situation than if the scenario descriptions were based on authentic settings and events.

In the following sections, we describe the different categories outlined above. The categories are often further divided into different sub-categories. These are outlined while we simultaneously explain the choices that we made which gave the categories their current form.

5.1 Geography

As the Piql Preservation Services is a service which is meant to be employed by users all over the world, it was necessary to break the category world geography into more manageable groupings. We therefore operate with three geographic zones: North, Middle and South. As a way of dividing the world into these zones we chose to base the classification on three indicators: climate, developmental level and political stability. Climate was chosen as the main classifier, as we deem this to be the most stable indicator over time, even considering climate change.

The zones will serve to illustrate that a risk to the Piql Preservation Services outlined in a scenario which takes place at one location in a given zone could easily occur in another part or country of that zone.[5] For example, a scenario describing a tunnel fire in China can easily be applied to any other setting with similar conditions. piqlVaults in the same zone would be exposed to many of the same types of natural disasters and many of the same vulnerabilities where it comes to utility supply and issues of political stability. Additionally, we aim for this classification to be useful also to the users of the Piql Preservation Services. By determining which zone a potential new Piql partner belongs to, it can easily see which threats and hazards may threaten their storage facility, and thus get an indication of what to include in its own risk and vulnerability assessments.

[5] Regional differences will, of course, occur, as the zones are necessarily wide and sweeping to simplify the scenario development.

The three indicators used to make the classification were chosen because together they comprise an adequate description of the characteristics of a country. Climate describes the relevant pieces of information needed about the geographical setting; developmental level encompasses aspects such as economy, education and health; and political stability incorporates issues of government and politics, and to an extent, past history, culture and demographics.

The decision to include these indicators instead of others was inherent to the nature of the Piql Preservation Services and thus the threats and hazards it might face. Including climate is important to take into account hazards threatening the physical properties of the piqlVault, piqlBox and piqlFilm. Developmental level and level of political stability was chosen in order to establish, first, the different kinds of threats most likely faced when storing varying degrees of sensitive information, and, second, what kind of safety and security measures one could expect to be present in the vault. It is, however, important to keep in mind that what classifies these indicators for a given zone today may not be the same in 200 or 500 years. Climate change may have a negative effect on the climate in a region; changes in world trade and economy may increase one country's developmental level while decreasing another's; and world events may significantly alter the political stability of a country. Such radical changes in the settings surrounding our object of study are matters we need to be aware of in our risk assessment. Yet, we cannot base our assessment on guesswork and fortune telling: we must base it on what we know to be true today and likely trends in the future. That is why the indicators are described according to the present circumstances.

Table 5.1 presents the details of the indicators for the different zones, including the potential hazards and threats associated with that indicator most likely to harm a piqlVault in a given zone.

Zone	Example regions	Climate	Developmental level	Political stability
NORTH	North America (US, Canada), Europe (Including Russia), East Asia (China, Japan).	*Temperate and subarctic*. Annual mean temperature (approx.): 10°C. Possible hazards: Earthquake, volcanic activity, flood, hurricane, tornado, tsunami, drought with extreme (high) temps, blizzards with extreme (low) temps, avalanche.	*High*. Strong economy, sophisticated infrastructure, stable energy supply (generators readily available), high standard on road network, sophisticated Ecom networks, high degree of law and order, proper crisis management. Possible hazards/threats: Loss of utilities (seldom), theft, espionage (many attractive targets), sabotage (many attractive targets).	*High*. High degree of accountability to population (-China, Russia), absence of violence/terrorism (-China, Russia, US, parts of Europe), high government effectiveness (-Russia), rule of law (-China, Russia), control of corruption (-China, Russia). Very stable borders. Possible threats: Terrorism (seldom), insider theft in low-scoring countries.
MIDDLE	Northern Africa (The Sahara, the Sahel, Sub-Saharan Africa), Middle East, Indian subcontinent.	*Subtropical*. Annual mean temperature (approx.): 25°C. Possible hazards: Sand storms, extreme (high) temps, flood, hurricane, volcanic activity, earthquake.	*Medium/low* (yet pockets of higher levels within countries). Weak economy (-Saudi Arabia), poorly developed infrastructure, highly unstable energy supply in certain countries (few generators available), low standard on road network, poorly developed Ecom networks, medium degree of law and order, unsatisfactory level of crisis management. Possible hazards/threats: Loss of utilities (high), loss of communications (high), theft.	*Low*. Low degree of accountability to population, incidents of violence/terrorism, low government effectiveness (- Saudi Arabia, Oman), little rule of law (- Saudi Arabia, Oman), poor control of corruption (- Saudi Arabia, Oman). Potentially unstable borders. Possible threats: Unstable borders, war, terrorism, theft.
SOUTH	South America Southeast Asia Southern Africa Australia	*Tropical*. Annual mean temperature (approx.): 20°C. Possible hazards: Flood, hurricane, extreme (high) temps, earthquake, volcanic activity.	*Medium.* Growing economy, adequate infrastructure, adequate energy supply, medium transport networks (fewer roads than railways), adequately developed Ecom networks, good degree of law and order, ok crisis management. Possible hazards/threats: Loss of utilities (medium), loss of communications (medium), theft, espionage (some attractive targets), sabotage (some attractive target).	*Medium.* Medium degree of accountability to population (worse in Southeast Asia), some incidents of violence/terrorism (-Botswana), adequate government effectiveness (- Argentina, Bolivia, Peru, India, Indonesia), low rule of law (better in Chile, Brazil, Botswana, South Africa, Namibia, India), problems with control of corruption (fewer in Chile, Uruguay, Brazil, Namibia, Botswana, SA). Stable borders. Possible threats: Terrorism, theft.

Table 5.1 Geographical zones. Sources: [19, 20, 21, 22]

5.2 Time Periods

With a longevity of 500 years, if not more, of the components of the Piql Preservation Services, the time perspective of the risk assessment in this project is a lot longer than what is normal. In fact, it is too long to be relatable. Consequently, we have created two time periods to use in the scenario development: one short-term and one long-term. The classification is again based on the users' needs, in this case how long we imagine a user would have need of the information which is stored. It was natural, then, to set the short-term time period from 0 to 30 - 50 years. This is the length of a person's career, and thus signifies the amount of time they can imagine needing access to information. We presuppose that the same goes for a business, as things will have evolved and changed quite a bit during this time, perhaps to the point of making the information obsolete. Any need to store information beyond this short-term time period we presuppose is for the preservation of the information for future generations. For instance, there is the need to preserve the cultural and historical heritage of a society, or the need to preserve original data for future research with new methods and ways of thinking. This long-term period is set from 50 to 500 years.

In the scenario descriptions, using the template as a tool, we describe whether or not a given scenario could take place in the present or whether it is set in an imagined future setting with different circumstances than today. If the latter is the case, what this indicates is that a given scenario could take place from that point in time onwards. Another presumption we have made is that a scenario which could take place today can also take place for the whole 500 year timeline.

5.3 User Class and Asset

The user groups that would be likely to utilise the Piql system for their archival needs have been defined into groupings. It is first necessary to briefly specify what *type* of information the Piql Preservation Services would be storing. It is not meant for keeping information which one needs access to on a regular basis and which must be backed-up regularly as new information is added continuously. Once this sort of information has been stored in internal archives for a period of about 5 years, it no longer needs to be part of the so-called active archive [23 § 3-12]. At this point, if the information is of such importance that the data owner wishes to preserve it, they can utilise the Piql Preservation Services.

As our working-perspective in the report is user-oriented, the user group classification needs to be as accurate as possible, yet it is one of the most challenging ones to define. The Piql Preservation Services is available to any entity in any sector or industry in the world in possession of critical data requiring archiving and long-term preservation. This includes the vast majority of all enterprises or bodies functioning in modern society, both private and public. Attempting to make a complete list of all these entities is near impossible. So, we have made a highly overarching classification of the user classes utilised in the scenario development. The groupings are based on the type of information, or asset, a given user would need stored and protected and the corresponding value, or degree of sensitivity, of that information. Defined in very broad terms, the user class is divided into the business or public sectors, storing sensitive or non-sensitive information. A new potential Piql partner can quite easily locate the user class within which it belongs, and thus gain a generic understanding of which risks apply to their organisation and which corresponding security measures should be put in place.

The level of sensitivity of the information is further divided into sub-categories. A measure of sensitivity is how critical its loss would be. The degree of sensitivity can vary greatly depending on how important the information is from one situation to another, from one period of time to another, and sensitivity is also often a matter of subjective judgement. As a frame of reference, we have chosen to use Norwegian legislation detailing which rules and regulations apply to different levels of sensitive information. Similar legislation can be found specifically for other nations. For the purposes of this report, the levels of sensitivity are divided into five groupings, outlined in table 5.2 below.

Sensitivity level	Description
Public highly sensitive	Classified or confidential information, as specified by national acts on protective security services [18].
Public sensitive I	Information exempt for public consumption, as specified by national regulations governing access to documents in the public administration [24].
Public sensitive II	Proprietary information, as specified by national regulations governing the management of information in need of protection for other reasons than those mentioned in the national act on protective security services, including regulations [25].
Business sensitive	Business confidential or proprietary information, as specified by the individual enterprise.
Public sensitive and business sensitive	Personal data, as specified by national acts regulating the processing of personal data [26].

Table 5.2 The classifications of sensitive information

Information that falls within the category non-sensitive is kept separate from the overview in table 5.2, as it solely depicts the various degrees of sensitivity of information which has already been deemed sensitive. Most of the digital information generated today is non-sensitive, and this category will undoubtedly comprise most of the information which is stored with the Piql Preservation Services. It is not to say that this information is not valuable and in need of long-term preservation: it is simply not sensitive, understood as information not needed to be withheld from the public. Non-sensitive information can certainly be valuable, such as the very high value cultural artefacts have to a society. Preserving the cultural heritage of a society is vital to uphold and safeguard the collective memories of what defines that society. Important historical documents, for instance, serve that function, and are thus highly valuable, and in need of sophisticated protection, yet they cannot be characterised as sensitive.

Now that the sensitivity of the information is more clearly outlined, it is possible to present a schematic overview of the user class defined by the asset and the corresponding sensitivity of the assets and therefore value of the asset. Additionally we give examples of the specific user groups which comprise a user class, shown in table 5.3.

User class	Level of sensitivity		User group	Asset
Business	**Non-sensitive**	Non-sensitive	Media – Entertainment, TV, film, newspapers.	Entire stock of past releases.
			Manufacturing – Machinery/equipment; Technology.	Supporting, consultative and contractual documents relevant to day-to-day work. Non-sensitive correspondence.
	Sensitive	Business confidential, proprietary information	Industry – Energy and utilities; Oil/gas; Chemical; Mining; Hydraulic power; R&D and production.	Trade secrets, possible threats to national interests. Contracts, deals, strategy papers, correspondence, financial data, product plans.
			Services – Ecom; Bank/Finance and insurances; Transportation; Satellite-based services; Health services: Estate agency business.	Trade secrets, possible threats to national interests. Contracts, deals, strategy papers, correspondence, financial data, product plans.
		Personal data	Any registered enterprise which employs staff.	Employee records containing personal information.
Public	**Non-sensitive**	Non-sensitive	Documentational purposes – National archives; National/public libraries; University libraries.	Historical, cultural & religious documents for future preservation. Used both for future research and a continuation of tradition/values. Cultural monuments.
			Public services – Social services; Public schools and universities; Health services; Property management.	Supporting, consultative and contractual documents relevant to day-to-day work. Non-sensitive correspondence.
			Fundamental research – Universities; Research establishments; Hospitals.	Research results.
			Legal – The judiciary, courts of law.	Law books, acts, statutes, verdict and settlement collection, legal treatises.

User class	Level of sensitivity		User group	Asset
Public	Sensitive	Personal data	Public registry of personal data – Social services; Universities; Finance/Insurance; Health services; Fire department; Police department, criminal records.	Documents relating to casework. Personal data.
		Proprietary information	Government administration – Government bodies; National archives and libraries.	Government records, central administration management, correspondence. Classified information. Internal case documents.
		Exempt from public consumption	Government administration – Government bodies; National archives and libraries.	Government records, central administration management, correspondence. Classified information. Internal case documents.
		Classified, confidential	Defence and Intelligence – Military bodies and archives; Intelligence and security bodies and archives; Research establishments; Suppliers.	Classified information.

Table 5.3 The user classes and corresponding assets used in the scenario development

5.4 Location and Description of Storage Facility

Giving a description of the piqlVault and its surrounding environment that is accurate, precise and which reflects the way Piql AS envisions the implementation of the Piql system is an important step of risk identification, which will in turn let us give meaningful results in the analysis and evaluation phases. Of course, such a precise and realistic description of a piqlVault and its surroundings would vary greatly between countries and between sectors. So, we are required to create a simplified version of reality and of the Piql storage facility in particular. One representation of a piqlVault is presented in the following. This description does not serve as a requirement specification for the design of a piqlVault: it is merely meant to serve as a tool for the scenario development. A schematic presentation is given in table 5.4 below.

Type of storage facility	Location	Placement	Size	Operations	Storage conditions
piqlVault in office or industrial building	In a city, a well-populated area.	Placed in a basement or lower floors.	86 m². Holds 20.000 piqlBoxes or 2.240 terabyte (TB).	Automated handling and storage of the piqlFilms in the piqlVault. Machinery, special components of the system and personnel.	With power supply: 21°C, 50 % RH (ISO 18911:2010). Without power supply: Differs between geographical zones.
		Placed in the upper floors.			

Table 5.4 The location and layout of the storage facilities used in the scenario development

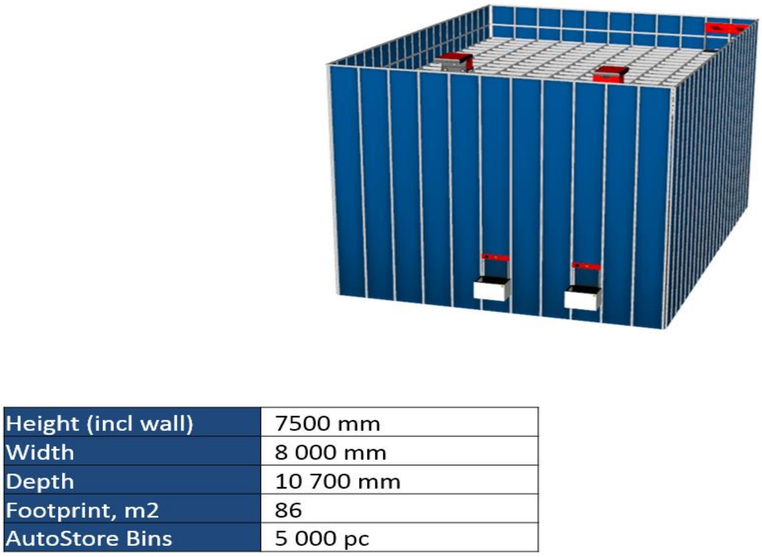
The storage facility used for analysis in this assessment is placed in one location: in an office or industrial building, depending on the user's needs, which is situated in a densely populated urban area. The choice of this location reflects the needs and circumstances of the user base of the Piql Preservation Services, which is mainly commercial.[6] Further, we have specified two possible placements of the storage room within the building: whether it is placed in the basement or on the lower floors of the building, or higher up on the upper floors. This has significance for different types of risks the storage room is exposed to. For instance, a storage room placed in a basement or in the lower floors of a building would be less vulnerable to shakes in case of an earthquake, but more likely to suffer heavy losses in case of a flood. Conversely, the storage room placed in the upper floors would be less vulnerable in case of flood, but more likely to be harmed by an earthquake.

We have defined a standard size for the storage room within which the piqlVault is placed that applies to all scenarios. The room has a surface area of 86 m², with a width of 8,0 meters and a depth of 10,7 meters. The height is 7,5 meters. The ideal storage conditions for the piqlBox and piqlFilm in order to guarantee the longevity of 500 years is 21° Celsius and 50 % relative humidity to avoid condensation [27, 28].[7] This is in accordance with ISO standard 18911:2010, according to which longevity testing has been done in earlier R&D projects. The automated storage system used in the piqlVaults is also compliant with these regulations. For the sake of continuity, it will also serve as the baseline storage conditions from which the scenarios are developed.

[6] It should be noted that users who wish to store and preserve more sensitive, or in other ways particularly valuable information, understandably may not view a regular office building as providing sufficient safety and security. These users can instead place the piqlVault in a mountain repository. More on this is chapter 10.

[7] More specifically, the stipulation is to maintain a temperature in the range of 4 – 21°C and a relative humidity in the range 20 – 50 %.

In coordination with Piql AS, it has been decided that all storage facilities evaluated in this assessment are fitted with a fully automated storage system, a modified version of Element Logic’s AutoStore® system. This system is used for the automatic handling and storing of piqlFilms in the piqlVault.[8] Within the space described above there is room for an AutoStore® grid which holds 5.000 piqlBins, each containing four piqlBoxes stacked horizontally on top of each other. This puts the total at 20.000 piqlBoxes, or 2.240 terabyte (TB) worth of digital storage space.[9]



Height (incl wall)	7500 mm
Width	8 000 mm
Depth	10 700 mm
Footprint, m2	86
AutoStore Bins	5 000 pc

Figure 5.1 The size and layout of the piqlVault system. Source: Piql AS

The modified version of the AutoStore®, from now on referred to as the piqlVault system, and how this automated system operates, is described in the following. This includes what we alluded to in chapter 3, namely the control system of the piqlVault system, or the data input, the physical handling of the piqlBins, done by robots, and lastly the external structural dependencies, such as power supply, and where in the system this is critical. The IT system security architecture is described further in the last section of this chapter.

[8] According to Piql AS’s wishes, the report only assesses risks in a piqlVault with an automated storage system. It should be noted, however, that it is likely that some users would not wish to utilise this operating system, preferring instead a manual system for handling the piqlFilms.

[9] The specifications on the storage capacity in the piqlVault for the purposes of this analysis was as part of an email correspondence with Katrine Thomsen, Project Manager at Piql AS, on 07.10.2015.

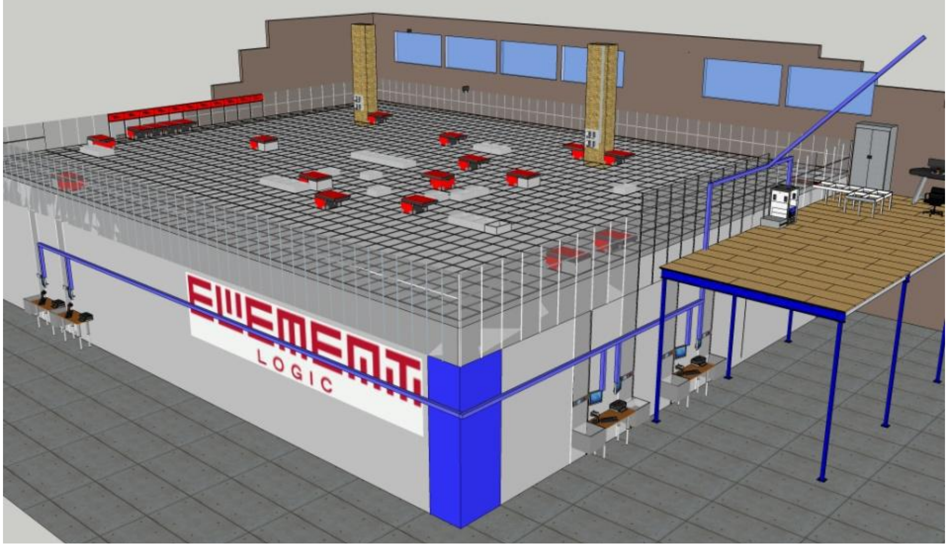


Figure 5.2 The operations of the piqlVault system. Source: Element Logic AS

The main structure of the piqlVault system is an aluminium grid which can be expanded upon demand. Within this grid, piqlBins are stacked on top of one another, a feature which adds additional stability to the otherwise quite sturdy structure. There is minimal electronic presence inside this grid. Most of the electronics are located at the top of the grid, where robots – in the case of the piqlVault system outlined above: two robots – zoom around. The robots run on batteries which last for about a day. Near one end of the grid, there are charging stations, where the robots can charge its batteries. Attached to the grid, there is a service mezzanine where the robots are offloaded for repairs. The robots require very little electricity, meaning that the risk of electrical fire, though present, is not as high as one would assume with a fully automated system. Neither is the amount of heat dissipation.[10]

Upon request, the robots pick up the correct piqlBins containing the piqlBoxes which were ordered and transport them to an operator port where a human operator can retrieve them. The movement of the robots is managed by a Controller, which must be situated onsite on the service mezzanine connected to the gird. The Controller sends commands to the robots through radio signals telling them which piqlBins to pick up and where to deliver them. The robot then lowers a lifting unit attached to it down into the grid to retrieve the indicated piqlBin, but the electronics involved in this process are minimal, so there is very little fire hazard. Piql AS has also made a backup plan for manually extracting the piqlBins in case of prolonged power failure [29]. After having retrieved the correct piqlBin, the robot delivers it to the correct operator port. This is the second location in the system where there is a concentration of electronics, with sensors, “normal” computers and barcode readers. A redundant energy supplier is not part of the standard outfit of the piqlVault, but this is possible to facilitate into the piqlVault system. There is, however, a backup generator which lasts for 24 hours.

[10] See appendix C.1.

The Controller which sends the commands to the robots has no knowledge of which piqlBoxes are in which piqlBins, only where each piqlBin is located at any given time within the grid. It is the Element Logic Warehouse Management System (EWMS) which contains these details. The EWMS stores all information regarding the location of a specific piqlBox containing a specific piqlFilm, which is linked to a unique reel ID stored on a hard disk directly shared with the Piql IT system.

5.5 Safety and Security Requirements

As the design and layout of the storage room used for analysis is described, it is possible to specify which safety and security requirements are built into the storage facility.

In order to become a certified provider of the Piql Preservation Services, meaning providing the services under conditions guaranteed to ensure the preservation of the data for at least 500 years, both with regards to their longevity and their security, a Piql partner must adhere to certain requirements as stipulated by Piql AS. A minimum level of such requirements has been defined by Piql AS with regards to specified storage conditions, which includes protective safety measures, and to physical security. These requirements are laid out in the document entitled “PiqlVault Storage Conditions and Security Requirements” [27]. In the next two sections of the report we will describe these requirements for safety and security considerations, and outline how they will be used in the scenario development for this assessment. Some of the requirements are very detailed both in their specification and description of implementation, whereas others are not as detailed and have required some additional descriptions from us. Here, we have made some assumptions for the purposes of this assessment. These are outlines in the schematic presentations of the requirements which follow each description of the requirements from Piql AS.

5.5.1 Safety Requirements

The piqlVaults will, as previously stated, be placed in standard office or industrial buildings. Safety requirements as defined by law vary greatly between countries, depending on the risks associated with a given geographic location. In addition to observing the national legislation and regulations governing safety requirements in building design and construction, Piql partners are required to fit the Piql storage facility with additional safety measures.

Safety requirements in a building structure serve as mitigation measures against accidents or natural disasters and sometimes deliberate attacks. Such measures can include fortified walls, fire protection, water protection, redundancy in utility supply, seismic resistance measures, and in especially reinforced structures, it may also include protection against electromagnetic pulses and protection against radiation. This list is not exhaustive.

When it comes to safety requirements, Piql AS describes a quite detailed regime. Here is a sample of the most relevant ones for this report:

- The piqlVault shall have flame, heat and smoke detectors.
- The piqlVault should be protected by a fire suppression mechanism minimizing the use of water. As unattended fire sprinkles could lead to flood of the film, it is highly recommended to use oxygen reduction suppression solutions which create an atmosphere where the fire cannot break out but the oxygen levels still allow access to operators.
- The piqlVault shall have handheld extinguishers along the warehouse (Class A, B, C).
- The piqlVault shall have slightly positive air pressure to help keeping the dust away.
- The piqlVault should not have any gaseous impurities such as sulphur compounds, ozone, peroxides, ammonia, paint fumes, solvent vapours and other active compounds.
- The piqlVault shall be separated in a dedicated room without any other activity to keep the environment as stable and non-affected as possible. Avoid contaminants coming from other processes (e.g. ammonia from photocopying devices, ozone from industrial areas, etc.).
- The piqlVault should be located above basement levels in geographical areas affected by flood risk. Otherwise underground locations are recommended but require good humidity and temperature control.
- The piqlVault must have power redundancy system like power generators keeping environmental control systems up for extended period of time (days).
- The piqlVault physical facility should comply with national construction standards to protect building structure against seismic activity.

In table 5.5, we have made the following strategy for the implementation of the measures described by Piql AS for the purpose of analysis. Some descriptions directly reflect Piql AS' requirements, and others are technical assumptions. It must also be noted that different Piql partners will implement these safety requirements in different ways, depending on the means of the user and the developmental level of the geographical setting, as it implies which resources were available during the construction of the building.

5.5.2 Security Requirements – Physical Security

Built-in safety measures, such as the ones described above, are an important part of an overall protection scheme, but they are seldom sufficient alone to ensure the full protection of an object. One also needs external security measures which regulate such parameters as access control, camera surveillance, alarm systems and sensors and the number of security guards on duty. Together these elements make up what is termed physical security [30]. Access control includes both perimeter control which regulates access to the site or location of the facility, and protective barriers such as sluices, turnstiles, and access verification solutions for controlled areas which are meant to regulate the movement of persons once they are inside the facility. Camera surveillance generally covers critical points around and inside the facility 24 hour a day, such as exits and entrances, to facilitate real-time action and, if needed, later investigations.

Safety requirements	Implementation
Fire protection	Flame, heat and smoke detectors present in the piqlVault. Fire suppression mechanism: an oxygen reduction suppression solution is recommended. Handheld extinguishers present in the piqlVault (Class A, B, C).
Water protection	Recommended location of piqlVault above basement levels in geographical areas affected by flood risk. If not, underground locations are recommended. Fire suppression mechanism: an oxygen reduction suppression solution is recommended, as unattended sprinkles could lead to flood of the film.
Seismic resistance	Building structures housing the piqlVault should comply with national design and construction standards of seismic mitigation if geographical zone is prone to earthquakes.
Chemical and biological compounds	A slight positive air pressure present in the piqlVault. No gaseous impurities present in the piqlVault.
Power redundancy	No redundancy in energy supplier, but piqlVault must be equipped with power generators to keep environmental control systems up for at least 24 hours after main power failure.
Other influences	The piqlVault shall be separated in a dedicated room without any other activity to keep the environment as stable and non-affected as possible.

Table 5.5 The safety requirements of the storage facilities used in the scenario development

Alarm systems and sensors are also placed at critical points. They are in place as a deterrent to break-ins and also to alert the security personnel when set off. They also often create confusion and stress for the person or persons setting off the alarm. Security personnel also serve as a deterrent through their often highly visible presence. Their more important and prominent role, of course, is to serve as additional mobile security resources when a situation arises, who are able to adapt to situations as needed.

Piql AS has also formulated a security regime to be applied during the storage phase of the service journey, and one which applies during production and transportation. The regime is laid out in the same document as the safety requirements, and for the part which applies to security it is based on the Content Delivery & Security Association (CDSA) standard “Content Protection & Security Standard” [27, 31]. In the document, Piql AS specifies the necessary requirements of the security regime which have to be present in a storage room in order for someone to become a certified Piql partner. The specific implementation, however, of said security regime is not described: that is largely left up to individual Piql partner so long as it is compliant with the requirement.

For the purposes of the scenario development, FFI has created a strategy for the implementation of Piql AS' security regime. The assumptions that we have made for the requirements are not directly based on any particular set of rules and regulations, as these would oftentimes greatly differ between countries. We have instead tried to find an average describing the security regime that can be applied across sectors and across geographical zones. Naturally, if a Piql partner is subject to national legislation on protective security services, the regulations stipulated there must also be implemented. This means that the suggested strategy should serve as nothing more than guidelines and inspiration for how the production sites and piqlVaults should be protected against external threats.

The requirements stipulated by Piql AS in the document are numerous, and we include a relevant sample here:

- The piqlVault shall have an alarm system activated when operators are not on duty.
- The piqlVault shall control access to facility. It shall be segregated, secured and monitored to prevent unauthorized access.
- The piqlVault shall implement and maintain policies and procedures for visitor access. These should include details of visitor registration, search policy and escorted access to secure locations.
- The piqlVault shall employ guards, who shall be on duty whenever operators are not in the premises.
- CCTV should be installed and deployed at the warehouse access points and at the points of contact with the piqlFilm (receiving ports - automatic).
- Monitoring shall be carried out by a guard when operators are not on duty.
- Uninterrupted power supply (UPS) must extend to all security systems and sized appropriately for local conditions and business activities.

Security requirement	Implementation during storage
Access control	Protective barriers in the form of doors/sluices inside the facility which opens with authorised ID verification solutions.
Alarm systems	Alarm systems installed in connection with authorisation devices. Activated outside office hours. Summons security personnel.
Camera surveillance	CCTV coverage of outside entrance area, all access points and all critical points inside the facility. Recorded 24/7, and monitored outside office hours.
Security personnel	One (1) guard onsite outside office hours. Sound vetting procedures for all personnel (either security clearance or criminal record and credit check depending on sector).

Table 5.6 The security regime of the storage facilities used in the scenario development

It is apparent that these requirements can be grouped together into the four main parameters included in physical security as outlined above, namely access control, alarm systems, camera surveillance and security personnel. FFI has made a strategy to implement the security regime as set forth by Piql AS, specifically for the storage facility, which includes these parameters. The strategy is presented in table 5.6.

Piql AS has devised separate security regimes which apply during the transportation and production phases. With these additional regimes, the protection of the piqlFilms containing valuable information is accounted for from the moment the sensitive data is converted from its original form into nanofilm to the moment it is put in secured storage and onwards.

These are the requirements Piql AS has stipulated when it comes to the security regime applied during production [32]:

- The facility shall have control access [sic]. It shall be segregated, secured and monitored to prevent unauthorized access.
- The facility where rooms are located shall have an alarm system activated when operators are not on duty.
- CCTV should be installed and deployed at the facility access points and at the production rooms.
- CCTV Monitoring shall be carried out by a guard when operators are not on duty. When operators are in duty, recording mode shall be enabled.

At FFI’s suggestion, Piql AS has added the following stipulations regarding the security regime which should apply during the transportation phase [27]:

- General level of security from a professional trusted transportation security service provider is required.
- The films shall be labelled and scanned for constant tracking.
- The films shall be stored in a safe in the holding area, protected by a PIN lock.
- Personnel shall have gone through criminal background checks and driving record reviews.

Though the security requirements during transportation do not fall squarely into the parameters we have defined earlier as necessary parameters of physical security, we have decided, for the sake of continuity, to keep to the same categories as used in the strategy for storage in our implementation of the strategy for production and transportation, though the latter entails a few adjustments to fit the different settings.

Table 5.7 presents FFI’s strategy for the implementation of the security regime which applies for the production and transportation phases.

Security requirement	During production	During transportation
Access control	Production site only accessible with authorised ID verification solutions.	Armoured or otherwise fortified truck used by a professional and trusted transportation service provider. The doors are locked at all times.
Alarm systems	Alarm systems triggered by sensors installed in connection with locked doors outside office hours. Summons security personnel.	The goods are labelled and scanned for constant tracking. During the journey they are stored in a safe in the holding area, protected by a PIN lock.
Camera surveillance	CCTV coverage of access points and all production rooms from multiple angles.	The goods are under constant watch. The personnel are not allowed to leave the goods unprotected.
Security personnel	Guards monitoring the CCTV footage outside office hours. During office hours, the CCTV footage is merely recorded.	One driver and one additional security officer. Sound vetting procedures for all personnel (either security clearance or criminal record and credit check depending on sector).

Table 5.7 The security regime during the production and transportation phase

5.5.3 Security Requirements – Computer Security

As the Piql Preservation Services is both an online and offline commodity, describing only the physical security surrounding it is insufficient: we must also describe the architecture design of the IT system used by the Piql partners during the production of the piqlFilms, i.e. when the digital data received by a user, or client, is converted into the piqlFilm.[11] It is only during this production phase that the Piql Preservation Services are connected to external networks like the internet, but with relatively strong security mechanisms implemented. For the rest of the service journey, it is only the metadata extracted from the original files which can be found online.

This section is very much linked to the service journey as described in chapter 2, but here we give a more detailed description of the IT processes which are performed along the way in the service journey. Figure 5.3 provides a detailed graphic description of these processes, and we recommend following the flow of information illustrated here for ease of understanding.

The first step of the service journey is when the original files of the user’s digital data, from now on referred to as the client data, is ingested into the system of the Piql Preservation

[11] At the time of writing, there is no Piql IT system in operation for FFI to study, merely a test system. However, after having received sufficient information on how the operational system eventually will be implemented, we here base our analysis on this description of the Piql IT system.

Services, or the Piql computer system.[12] The client data is depicted in red in figure 5.3. Piql AS' Front-End service or interface allows the client to transfer their data into the Piql computer system in one of two ways: the client can either upload the data to the Piql system using a secure connection through a public web server or manually deliver a portable hard-drive containing the files to the Piql partner. These options are depicted as two solid black lines going from the client computer interface to the Piql computer interface. The reader will notice that the black line denotes the logical transfer of data throughout the entire system.

Should the client choose to upload the data via the internet, the Front-End code provides secure connections through the use of HTTPS or S-FTP protocols to ensure secure communications between the client interface and the Piql interface. All communication happens within this encrypted connection. The HTTPS/S-FTP connection is the standard solution offered by Piql AS as the Front-End service. However, should the client require it, additional security can be added through an OpenVPN. The Piql partner then sends the setup for the OpenVPN to the client, which contains certificates and necessary keys. When the client installs this setup, a cryptographically secure tunnel is opened between the client and the Piql partner which exists in addition to the HTTPS/S-FTP connection already in place.

The Front-End code also includes a Squid reverse web proxy, a feature which allows an unlimited number of clients to reach a designated web server, in this case in the Piql computer system. Only requests made to this web server are forwarded, while requests that are not according to HTTPS are at the same time detected and terminated.

The entire Front-End service runs behind a firewall, which by default rejects all traffic to the Piql computer system unless it comes through designated ports. Once the data is allowed to enter into the external interface of the Piql computer system, there is additional security in place which monitors and analyses real-time all the traffic which passes through. Such a Snort intrusion prevention and detection system is there to make sure that all of the other security measures just described have done their jobs [35, 33].

Upon receiving the client data, the Piql computer system performs additional security checks on the digital data, which includes a virus check and an internal integrity check. The latter is to make sure that none of the client data was altered during the transfer into the Piql system. Simultaneously, the Piql computer system begins processing the client data: collecting and storing metadata from the files to enable future access (depicted in green in figure 5.3); encoding the files into Piql format based on the preferred method of preservation (digital, visual or hybrid); and creating a checksum of the original file for later reference. The checksum and the original file are kept separate throughout the remainder of the process.

[12] For those interested: Piql AS' operational IT system is based on open source industry best practice components. The Piql computer, which manages all the tasks in the workflow, uses an open source LAMP stack (Linux, Apache Web Server, MySql and PHP). For more, see [33, 34]

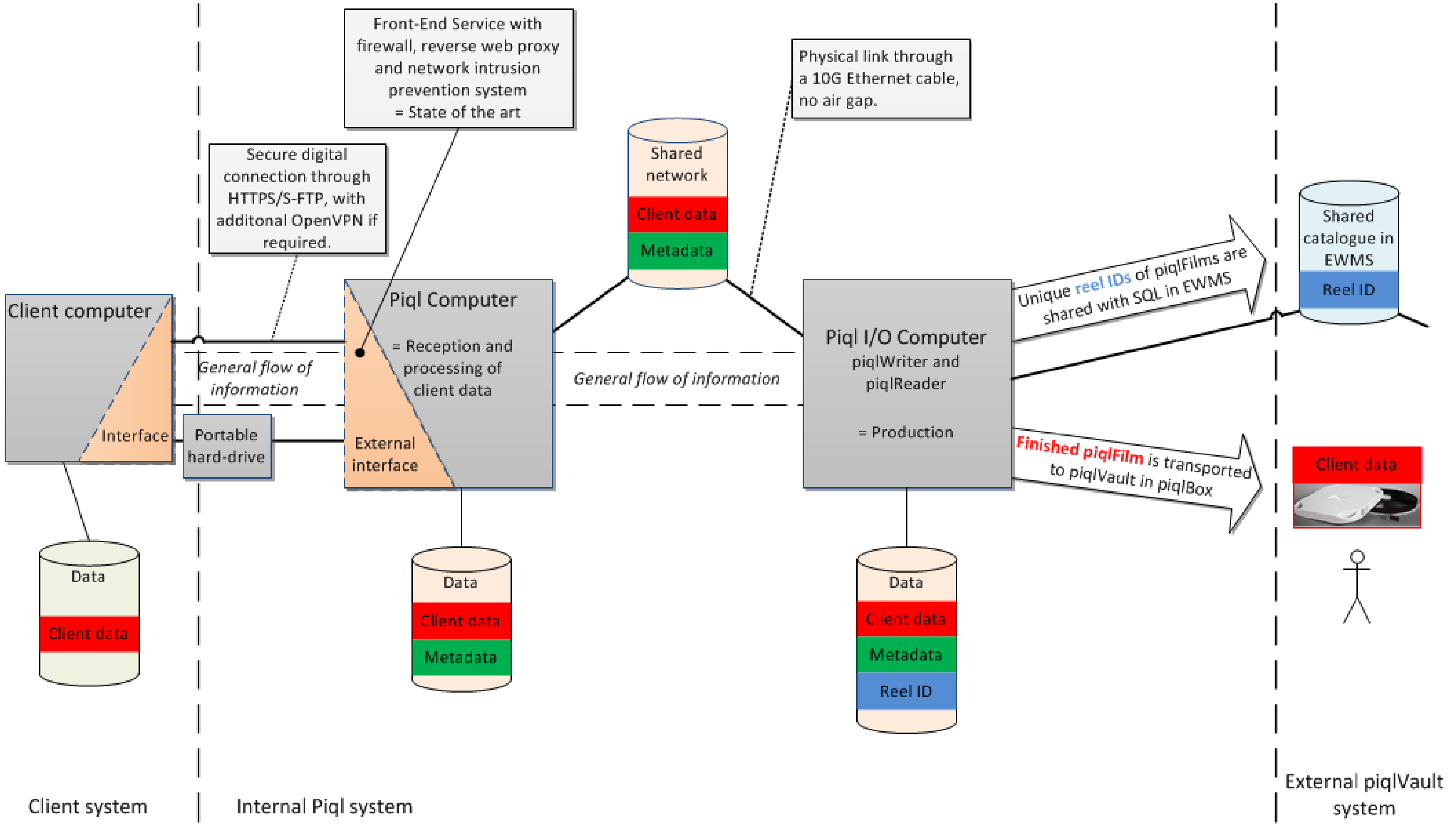

Client computer
Interface
Data
Client data
Secure digital connection through HTTPS/S-FTP, with additonal OpenVPN if required.
General flow of information
Portable hard-drive
Front-End Service with firewall, reverse web proxy and network intrusion prevention system = State of the art
Piql Computer
= Reception and processing of client data
External interface
Data
Client data
Metadata
Shared network
Client data
Metadata
General flow of information
Physical link through a 10G Ethernet cable, no air gap.
Piql I/O Computer
piqlWriter and piqlReader
= Production
Data
Client data
Metadata
Reel ID
Unique reel IDs of piqlFilms are shared with SQL in EWMS
Finished piqlFilm is transported to piqlVault in piqlBox
Shared catalogue in EWMS
Reel ID
Client data
Client system
Internal Piql system
External piqlVault system

Figure 5.3 The Piql IT system security architecture

Once the processing is done, the prepared file in Piql format is stored on a shared hard disk between the Piql computer and the Piql I/O computer. The shared hard disk is utilising a Network File System (NFS), which is a distributed file system allowing several servers access to certain files. This is the manner in which the prepared file is transferred between the Piql computer and the Piql I/O computer, shown in figure 5.3 as where the black line moves between the computers via the NFS. The physical interconnection is through 10G Ethernet cables, i.e. there is no air gap between the computers.[13]

The file with the processed client data is then written onto the piqlFilm. After the film is developed and processed, it is read back on the piqlReader to verify its contents against the checksum generated for the client data when it was first uploaded to the Piql system.

As the client data is now converted into its physical form, the digital client data is no longer needed. It is deleted from all computers in the Piql IT system, and only the metadata collected earlier in the process is connected to external networks. Additionally, a unique film reel ID is generated once the piqlFilm is printed. Figure 5.3 depicts this newly created information as blue. The unique reel ID is stored on a shared catalogue with the database in the Element Logic Warehouse Management System (EWMS), the control system of the piqlVault system, while the finished piqlFilm is labelled, packed and transported to the storage facility.

Separated from the specific processes and steps of the production, but equally important to consider when designing the security infrastructure of an IT system, are the measures put in place to mitigate the threat of the insider, i.e. operators of the Piql computers and components or other personnel who can, for whatever reason, cause damage to the client data. The Piql complete IT system is designed so that regular operators have no access to client content: only administrative users have this access. This is enforced by the design of the operator interface controlling the workflows. The machine design is another measure. For example, the cover of the piqlReader must be down during the scanning of data so that the operator cannot see what is being scanned [33].

Piql does not provide protection in the form of encryption of the data to its clients. The information on the piqlFilm must remain readable without a separate key to break the encryption, as the PiqlFilms are supposed to be self-contained, i.e. that they can be found in 500 years and all the instructions needed to read the information again is stored right there on the first few frames of the piqlFilm. The client, or user of the Piql Preservation Service, does of course have the option to encrypt the data themselves before transferring the files to the Piql partner. Yet this is not part of the Piql partner’s service: the users do this at their own cost and risk, and they are themselves responsible for managing the personal key.

Figure 5.4 illustrates the next steps the digital data take after being processed in the internal Piql IT system. It explains the architecture design of the IT system used in the piqlVault system

[13] The specifications regarding the physical interconnection was as part of an email correspondence with Ole Liabø, Director R&D at Piql AS, on 24.02.16.

during the storage of the piqlFilms. The two systems are linked, as the information is transferred electronically between them.

In figure 5.4, the entirety of the internal Piql IT system is condensed into one frame which shows the metadata and the corresponding reel ID still stored in the system, and the corresponding client data in its offline physical form ready to be transported to the piqlVault. The only logical information shared between the Piql IT system and the piqlVault IT system is, as also shown in figure 5.3, the unique reel IDs stored on a shared hard disk with the control system of the piqlVault system, the EWMS. The physical information, the piqlFilms containing the client data, is transported from the production site to the piqlVault after being properly packed in piqlBoxes and labelled. Once the piqlBoxes containing the piqlFilms arrive at the piqlVault, they are manually ingested into the piqlVault system. During this process, operators link the piqlFilms- and Boxes to the digital reel ID which is already stored in the EWMS and insert them into the grid at the operator ports for the robots to pick up and store at designated locations.

The main purpose of the piqlVault IT system is to control the movement of the piqlFilms, i.e. the processes related to their ingestion and retrieval on demand. As figure 5.4 shows, the piqlVault IT system operates on three separated networks: the C network, which is the Piql IT network; the B network, which is the interface network; and the A network, which is the piqlVault system network where most of the processes related to the workflows of the piqlVault system are handled.

The C network is the Piql IT network described above. The B network serves to connect the Piql IT network (C) and the piqlVault system IT network (A). This is where the shared catalogue of reel IDs is placed on the EWMS. Its server is password protected, and the different user accounts also have restricted access to the contents on the server. When a specific piqlFilm is requested for retrieval, the EWMS locates the correct piqlBox identified by the unique reel ID in its system. As an example to illustrate the process, we can image a reel ID with the signifier reel ID P.367. After having located this reel ID, the EWMS then matches it to the local piqlVault ID A.102, another imagined example. These local IDs were created when the piqlBoxes were ingested into the PiqlVault system, and signifies its position in the piqlVault grid. In figure 5.4 the local ID is shown in purple. The EWMS then forwards the request to be processed further on the A network.

The A network exists completely separated from the two other networks to avoid any signal interference from other processes going on simultaneously in the IT system as a whole [9]. It is used solely for the operations of the piqlVault system, and its separation is vital both for the effectiveness of these operations and the security of the system. A highly important component of the piqlVault system is placed on the A network, the piqlVault system Controller, whose only job is to manage the movements of the robots on the piqlVault grid. It must be placed onsite in order to communicate with the robots. The Controller houses no information about the piqlFilms, neither their contents or their metadata, nor their reel ID. It only has a registry of the local IDs and information about the location of the piqlBoxes connected to the local IDs, both

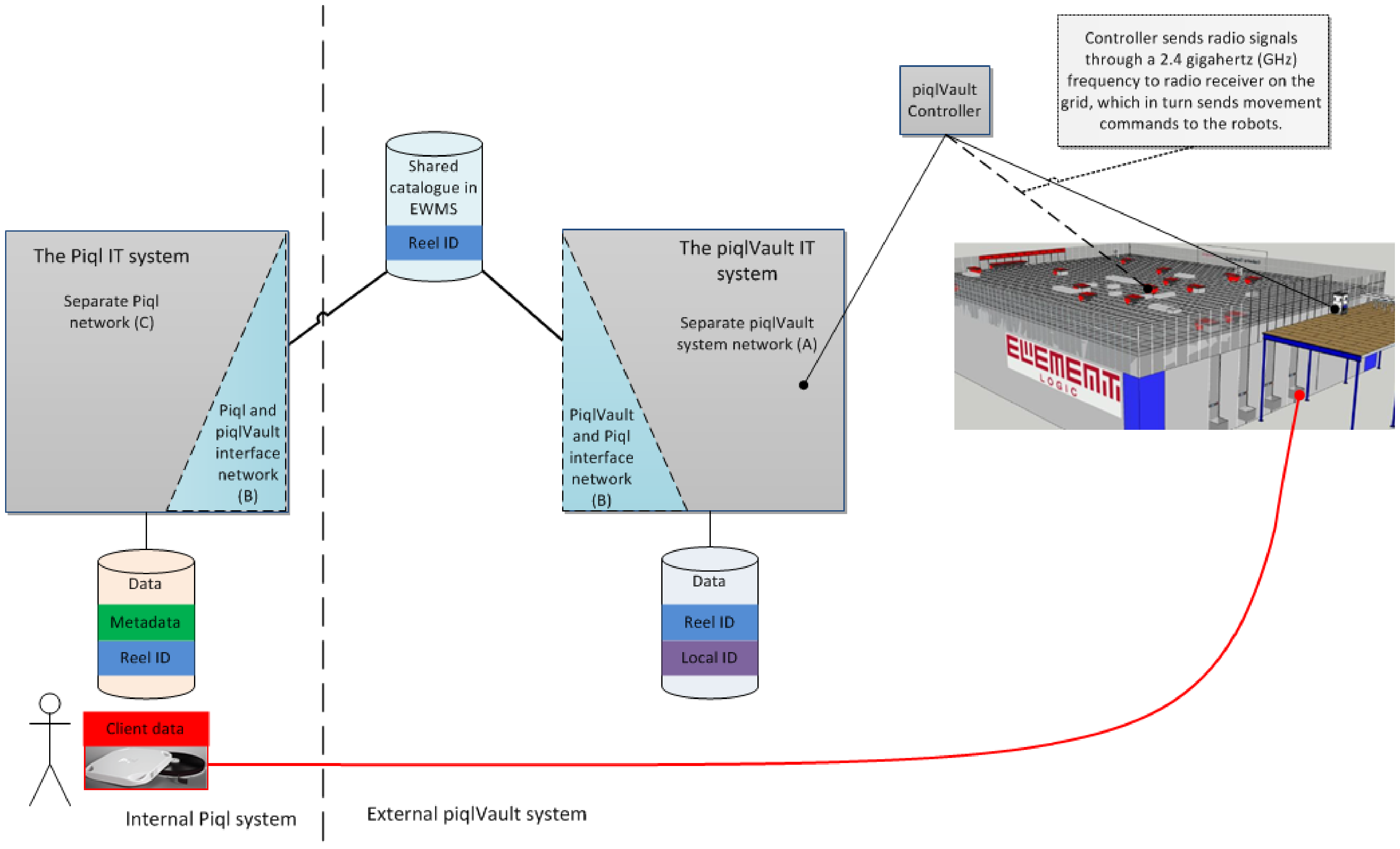

The Piql IT system
Separate Piql network (C)
Piql and piqlVault interface network (B)
Data
Metadata
Reel ID
Client data
Internal Piql system
Shared catalogue in EWMS
Reel ID
External piqlVault system
The piqlVault IT system
Separate piqlVault system network (A)
PiqlVault and Piql interface network (B)
Data
Reel ID
Local ID
piqlVault Controller
Controller sends radio signals through a 2.4 gigahertz (GHz) frequency to radio receiver on the grid, which in turn sends movement commands to the robots.
ELEMENT LOGIC

Figure 5.4 The piqlVault IT system security architecture

the piqlBin in which it is placed and the exact location of that piqlBin in the piqlVault grid. Our example of the workflow can thus be expanded upon: the EWMS receives a request for the retrieval of reel ID P.367. It then matches that reel ID to local ID A.102. The EWMS then signals the piqlVault Controller to pick up the piqlBin in which the piqlBox with the local ID A.102 is placed.

Having received the request for pick-up of local ID A.102, the Controller signals the robots to move to the right location and retrieve the correct piqlBin. These signals are radio signals sent through a 2.4 gigahertz (GHz) frequency[14] to two radio receivers on the grid, which in turn direct the signal to the robots. There are two radio receivers in case one of them is put out of commission for whatever reason. The radio signals from the Controller to the robots contain no information regarding what is in the different piqlBins, simply their location as specified by coordinates. The security protocol used by these radio signals is a protocol of the supplier of the AutoStore® system's own design, the contents of which FFI has not been privy to.[15]

Finally, the robots, having picked up the correct piqlBin containing the correct piqlFilm with local ID A.102, take the piqlBin to an operator port, where a human operator retrieves the piqlBox with the reel ID P.367. The piqlBox can now be transported wherever it is requested to go.

6 Selection of Scenarios

6.1 Scenario-Based Approach

Our assignment is to assess the threats and hazards that may harm the Piql Preservation Services today and for 500 years to come. With a timespan of this magnitude, many possible futures are conceivable, and the degree of uncertainty tied to which of these futures will come to pass is quite large. What we do know is that these futures consist of a huge array of possibilities, some of which will have great significance for our circumstances should they become reality. Examples include the negative effects of climate change, the manifestation of artificial intelligence, and so-called black swans. The term black swan refers to an event no one imagined could happen, yet one that did occur after all and its consequences were dire [36]. Although we cannot predict exactly what will happen, especially when considering less likely yet serious

[14] Currently, the system uses a 433 GHz frequency. Element Logic will shortly switch to 2.4 GHz, so this is the frequency we use as a basis for analysis.

[15] The information regarding the connection between the Controller and the robots was given during a meeting with Terje Skjølberg, Sales Manager at Element Logic AS, on 11.11.15.

events, we can plan for *something* happening, and in that way help minimise the negative consequences if they do [37].

The scenario-based approach is a method used to help us model and manage this uncertainty. It is one of the most used foresight techniques in Norway, implying that its usage is very well-founded, which is the case at FFI. The scenario-based approach lets uncertainty serve as a guide when structuring possible future events, as opposed to other methods, such as prognosis-making, which instead only tries to minimise it. In this sense, we are liberated from only examining the developmental trends we can observe today. Instead, we are prompted to consider questions such as: How likely or unlikely is it that X event will occur in Z years? And even if it seems unlikely, should it occur, how significant will the event be for the object we are analysing? [38 p.162-179] Using this line of thought allows us to attempt to capture the outliers and account for such events which have a low likelihood but significant consequences. We are thus allowed to cast a wider net than would have been possible if we only used observable developmental trends and projections of actual progress as our sources of information in futures studies.

At the same time, the criterias for scenario development is that the scenarios are plausible, relevant and internally consistent. Plausibility infers that the scenarios must be grounded in reality and tangible facts, insofar as they must be able to take place in the real world. Relevancy implies that the scenarios are related to the subject of analysis. Developing a scenario is not in itself sufficient. It is only relevant insofar that it can be used as a tool put towards a bigger purpose, e.g. as a method for an analysis. Lastly, internal consistency refers to how the scenario cannot be developed based on premises which cannot exist together, i.e. which are mutually exclusive [38 p.162-179, 39 p.7-8]. We will return to the criterias for scenario development and elaborate on them further in chapter 6.3.

There exists a subtle, yet important distinction between the terms scenario development, scenario description and scenario analysis, as briefly touched upon in chapter 4. For the purposes of this report scenario development is understood as the process of mapping all the factors which need to be included in a given analysis for it to be able to give meaningful conclusions. A step in the scenario development is selecting the relevant scenarios for the further analysis. In this project, we use a method called morphological analysis, the procedure of which – and the resulting scenario selection – will be described in detail in chapter 6.3. Scenario description is understood as the act of writing out a scenario, selected and defined during the scenario development phase. Lastly, scenario analysis is understood as the processes of utilising the completed scenario descriptions to analyse results, make conclusions and give recommendations suitable to the assignment.

The scenario-based approach allows us to analyse and include a great number of possible future events. This aspect is vital in this project because there are a lot of issues and elements which need to be covered by this analysis in order to make it complete. These will be elaborated upon in the following.

6.2 Considerations in Scenario Development

Several considerations create an operating environment for this assessment which is very comprehensive: The universal and global application of the service, the 500 year longevity of the piqlFilm, -Box, –Bin and some elements of the piqlVault, and the interconnected physical and digital nature of digital preservation. We permit ourselves, in this section, a summary of the vast number of variables present in this assessment, which must all be considered in order for FFI to be able to make meaningful conclusions and recommendations regarding the Piql Preservation Services. We therefore briefly outline these variables with the hope that it will enable the reader to better understand the grounds upon which we based the decisions made in the scenario development.

Before the variables, or considerations, are outlined, it is useful to introduce the criteria by which the Piql Preservation Services will be judged in the scenario analysis, i.e. how well the system and all surrounding protective measures hold up against unwanted external influence. As the asset we are assessing the protection of in the scenarios is the information preserved on the piqlFilms, it is evident that we are in the realm of information security. It is natural to judge the Piql Preservation Services on its ability to guarantee the three key security properties of information security. These are confidentiality, integrity and availability, easily remembered by the abbreviation CIA, as described in chapter 4.

In addition to cover issues of data security, the assessment must also include the physical security of the system. We therefore ask the question of how the information on the piqlFilms can be compromised, either through the use of digital malware which damages or extracts without permission the encoded information on the piqlFilms or because the physical components of the system – the film, the box and the vault – are physically damaged. Both incidences cause the information to be compromised, jeopardising the confidentiality, integrity and availability of the information that is preserved.

Additionally, the scenario selection must also consider various causes of a security situation challenging the Piql Preservation Services. The field of risk assessments is commonly separated into two concepts: safety and security. Safety is defined as protection against unwanted events that are caused by one or more coincidences, or unwanted unintentional events. Security is defined as protection against unwanted events that are the result of deliberation and planning, or unwanted intentional acts [11, 12]. In security, we have to account for threat actors and their intentions and capacities because we are referring to events that are premeditated and pre-arranged. This is unlike safety, where we cannot speak of threat actors in the same way. This is not to say that there can never be a human actor who instigates an event in the safety category. An accident can be a result of human error, but then the act is not deliberate, and the following situation cannot thus be characterised as being related to security. The selection of scenarios in our assessment must include issues that arise in both safety- and security-related situations, because both can have negative consequences for the Piql Preservation Services.

Another consideration to be kept in mind during the scenario development is the many phases the information goes through in the Piql Preservation Services Journey. The reader will recall the scope we have defined for the assessment, which includes the objects of study, the structural relationships between these objects and the defined security parameters surrounding it all. The scenarios chosen must firstly account for risks faced by the Piql Preservation Services during production. This entails risk that may harm the Piql system during the steps of receiving the data, the ingestion phase of the data into the piqlWriter, while the piqlWriter prints the piqlFilms and they are developed, and finally when the finished films are read back to verify their integrity and accuracy.

Furthermore, the scenario selection must include the transportation phase from the production site to the designated storage facility when the boxed piqlFilms are out in the open and more exposed to external influences.

Most of the scenarios must cover events that may occur while the films are in storage which may have consequences for the confidentiality, integrity and availability of the information. We assume that the piqlFilms can be stored in three different geographical zones, placed in different settings at their locations, and operated by an automated handling system. Additionally, the safety measures and security regimes that would be in place for the different user classes protecting information with varying levels of sensitivity must be accounted for. These variables too must be covered in equal measure in the scenario analysis.

The main challenge in the scenario development is finding a balance between all these variables and considerations, and making sure they are included in the scenario descriptions to such an extent as is necessary for us to be able to do a meaningful analysis.

6.2.1 Scenario Constraints

The scenarios relating to issues of safety will take place only during storage and not during production or transportation. During both the production phase and during transportation a natural disaster or accident which harms the piqlFilms can, of course, occur. However, there is little one can do to plan for this or prevent the films from being damaged by accidents or natural phenomena when they are “out in the open” like this, i.e. not in secured storage, as these things happen without warning and can simply be chalked up to “bad luck”. When considering that it is nearly impossible to plan for the protection of the film from such events, the assessment would have no value other than to say “these things do happen, tough luck”. The piqlFilm will always be more vulnerable out in the open. In storage, however, the Piql partner has control of the environment and can implement safety and security measures to offset the effects of the above-mentioned, i.e. this is where the scenarios have a user value to the Consortium.

Most security scenarios have the Piql Preservation Services as the target, i.e. we are describing direct threats to the system. Yet, in the scenarios relating to terrorism and a nuclear event, we find it too unlikely that the piqlFilm is the actual target to make a plausible scenario. The scenario selection method of morphological analysis used in this assessment does find these scenarios as relevant direct threats to the Piql Preservation Services: we have simply chosen not to describe them that way, as this seems implausible considering the current application areas of the Piql system. We have instead chosen to include the scenarios where the Piql Preservation Services is not perceived as the direct target, but nonetheless suffer as an indirect effect or cascade effect. The piqlFilm is simply collateral damage to another attack not directed at it.

Similarly, as the Piql Preservation Services is not the target in these scenarios and there is no direct threat present, it is difficult for us to give specific recommendations on how to mitigate that threat. Our only recommendation must therefore be: always be aware of your surroundings. Avoid high risk occupancies such as close proximity to chemical plants or refineries, or placement of the piqlVault in a building which is likely to be a terrorist target due to one of the other occupants, or in a city likely to be the target of a nuclear attack. Other recommendations regarding the dangers that threaten the Piql Preservation Services in such scenarios, such as fire protection, fortified walls to withstand tremors or explosives, are covered in the measures recommended in other safety scenarios.

The scenarios more than often describe a worst case scenario where a vital safety or security measure is missing. This is simply to illustrate how badly this can damage the Piql Preservation Services in order to underline the importance of protecting the Piql Preservation Services from such harm. It does not have to be a complicated or expensive measure: the important thing is that it is present. Often a minor measure can make all the difference, especially when it comes to issues regarding security. It can simply be about putting enough (minor) obstacles in the threat actor’s way to deter them from acting. There is often an easy fix to the problem as well, e.g. move a vault placed in an area with a higher risk of flooding to a higher floor to avoid flood damage. One should always take into consideration that such changes can lead to different kinds of vulnerabilities, such as, in this example, making the vault more vulnerable to the effects of earthquakes and tremors.

An important delimitation of our scenario analysis is that the scenarios will not examine the consequences of loss of information, i.e. how this may affect the company storing the information financially or with regards to its reputation. Our scenario description and analysis ends once the film is damaged or removed from the piqlVault without authorisation. The aftermath falls outside the scope of our assignment. Our aim is to assist in the definition of the safety and security measures that need to be in place to prevent said loss.

Finally, we must make one caveat regarding one of the security properties CIA. Normally, for the security property availability to be deemed compromised the information in question must be unavailable at a time when it is urgently needed, i.e. it is both time- and situation specific. However, as the scenario descriptions in this report are generic, we have found it necessary to redefine the usage of availability. Therefore, when we conclude that availability has been compromised in a scenario, we mean that the information simply cannot be accessed – regardless of the data owner’s need for it.

6.3 Scenario Method

To make a representative and accurate selection of scenarios, one which we can trust will cover most or all of the entire spectrum of risk against the safety and security of the Piql Preservation Services, we have chosen a method of scenario selection known as morphological analysis. Morphological analysis is described as a non-quantitative method to structure and analyse complex problems within a wide number of subject areas [39 p.7-8, 40 p.10]. This section will give a brief introduction to the process and utilisation of the method, after which morphological analysis will be applied to the research question in this report.[16]

Morphological analysis (MA) is best described as a collective term for a variety of different techniques, all of which have a common purpose: to establish a complete overview of all the possible aspects and solutions for a given problem [40 p.10]. The way the method accomplishes this task is by producing a set of scenario classes, defined as a set of challenges or a category of possible outcomes that have important common denominators and which therefore naturally belong together. In this way MA goes beyond the individual scenarios. It is close to impossible to create an infinite number of scenarios which satisfy the scenario criteria of being consistent, relevant and plausible, that can rightly claim to cover *all* risk to a certain entity. Instead, by creating these scenario classes, MA is a method to better map the sample space and ensure an adequate breadth in the scenario selection [40 p.9].

The goal is to ensure that all relevant challenges are represented without making the total set of scenarios unmanageably large. MA tries to extend the space for possible outcomes in order to reduce the risk of omitting important scenarios, however unlikely they may be [39 p.10]. Naturally, the more unlikely they are, the easier it is to overlook them, which underlines the importance of correctly applying a method, such as MA, which helps us avoid this mistake. In our risk assessment the uncertainty of which risks might harm the Piql Preservation Services is quite high, and it is absurd to believe that we are able to ensure coverage of *all* possible outcomes. History has taught us that there will always be developments and events that are not foreseen. The aim is simply to reduce the risk of leaving out important scenarios and developments, but the risk can never be eliminated completely [39 p.10].

Together the scenario classes represent the total space of possible outcomes for a given problem area. This means that there are no scenarios that cannot be assigned into one or another scenario class, and that there does not exist a scenario which falls outside of this space. The sum of scenarios is therefore meant to be both exhaustive and mutually exclusive.

As stated, the morphological method is a collective term for many different techniques. The technique which figures most promptly in this report is the morphological box. This technique consists of two phases – the analysis phase and the synthesis phase – each of which contains three steps.

[16] For a more comprehensive description of the method, see [41, 40, 39, 42]

The first step in the analysis phase is to concisely define the problem. From there the dimensions, or *parameters*, that best characterise the problem are identified. The last step in the analysis phase is to assign a range of relevant conditions, or *values*, for each parameter. It is important to ensure that the values are mutually exclusive and exhaustive for the given parameter, insofar as that is possible. Together, the parameters and corresponding values make up the morphological space, shown in table 6.1 as an example of a morphological matrix.

Parameter A	Parameter B	Parameter C	Parameter D	Parameter E
Value A1	Value B1	Value C1	Value D1	Value E1
Value A2	Value B2	Value C2	Value D2	Value E2
	Value B3	Value C3		Value E3
	Value B4			

Table 6.1 Example of a morphological matrix

The next steps belong to the synthesis phase. First, one does an internal consistency analysis of the morphological matrix. The matrix shown in the example here consists of 2 x 4 x 3 x 2 x 3 = 144 theoretically possible combinations. This number is too vast to comprehend from an analytical point of view, and, additionally, not all of the combinations, or pairings, are plausible. It is the purpose of the internal consistency analysis to weed out these implausible parings. One compares the values to one another, one by one, asking the question: if A1, is B1, B2, C1 and so on possible? Internally consistent pairings of the *values*, meaning pairs that would be possible in the real world, are thus identified and fed into a consistency matrix giving you the total range of possible solutions existing in you morphological space. This is called the solution space for your given problem. From there you feed the results of the consistency analysis into an IT tool, which defines all scenarios which find consistent solutions on all *parameters*, i.e. a scenario which could exist in the real world. The resulting list of scenarios is called the outcome matrix.

Finally, evaluating the scenarios using common sense, you see if any are similar enough to comprise a scenario class. The result is a final number of scenario classes from which you make specific scenario descriptions.[17] As a tool in this final process, FFI has developed a scenario template adapted to the PreservIA project, enabling us to more easily describe a larger number of scenarios. The template is presented in chapter 7.

Morphological analysis was chosen in this project because it a method to structure and analyse complex problems, and the purpose of the assessment in this report is indeed a complex problem. We found, however, that while the method was suitable to identify issues related to security, it was less helpful with issues of safety. The same difficulty arose when FFI researcher Sunniva Meyer undertook a task of similar, if not higher, complexity: to map all threats to the security of an entire nation [43]. She reflected that because the sample space of such a complex

[17] All the steps of the morphological box are defined in [39 p.9]

problem in turn needed to be so large, the parameters that were defined would have very different relevance for different parts of the spectrum of events which could somehow affect the object of study. While attempting to apply the method to the entire spectrum it was also revealed that it would either become too specific in places or too ambiguous and crude in others [43 p.12]. The same reflections are relevant to the problem in our risk assessment. That is why we have chosen to use the results from her morphological analysis as a basis for the identification of issues regarding unintentional events. We found, as Meyer did in her analysis, that when it comes to issues of security it is necessary to do another morphological analysis solely on intentional acts [43 p.14].

6.3.1 Applied to Issues of Safety

In order to create a typology of all events which could affect a nation's security, Meyer utilised a modified version of morphological analysis, where the only two parameters were *cause* and *primary effect*. The values assigned to each parameter are listed below in table 6.2 [43 p.13].

Cause	Primary effect
Meteorological phenomenon	Mass destruction
Geological phenomenon	Larger environmental damage
Cosmic phenomenon	Considerable material damage or economic loss
Biological phenomenon	Loss of societal functions
Technical errors	Lack of vital resources
Human or organisational errors	Public trauma
Politically motivated criminal acts	Weakened physical or psychological integrity
Economically motivated criminal acts	Limitations on national sovereignty
Usurpation of power/sovereignty	
Destructively motivated criminal acts	

Table 6.2 Matrix for analysis of scenario classes of unintentional events

The scenarios which materialised from this morphological box showed a quite clear distinction between unintentional and intentional events. Many of the causes and effects in the morphological box presuppose a threat actor with intentions and capacities, and would clearly have nothing to do with unintentional events. Many, however, are relevant for issues of safety, and these are the ones of interest to this report. Meyer identified the following scenario classes in the category of unintentional events based on the causes and effects outlined above: natural disasters, failure or malfunction, sudden illness and aggregated individual acts.

The two latter – sudden illness and aggregated individual acts – are deemed not relevant for this study because the risks they pose to the Piql Preservation Services are too implausible or irrelevant for its safety and security – key criterion in scenario development. For clarity we list what they include: sudden illness includes highly contagious diseases and diffusion of vermin or insects; and aggregated individual acts encompass such actions as over-usage, sudden change in buying pattern, mass absenteeism and mass movement. It is possible to theorise that a highly deadly plague wipes out the entire Norwegian speaking population, making the information stored in this language unavailable to non-Norwegian speakers with an interest to access it. However, it is highly unlikely such a relentless plague would ever exist. Additionally, the world is highly globalised, which means that languages are taught to people all over the world, and native speakers also travel all over the world. So, it follows that a plague which truly makes Norwegian a dead language would have to eliminate the entire world's population, in which case, the piqlFilms are wanted by no one. Similarly, the availability of information stored on piqlFilm would be compromised for a time by a long-lasting strike, but there are no recommendations we can make in this report, which is targeted at safety and security measures, which would help in this situation – indeed, the only advice one could give is to make sure the data owner is in compliance with national legislation and regulations related to the working environment – i.e. such scenarios can give no significant insight into the vulnerabilities and security challenges of the Piql Preservation Services.

The two former scenario classes identified by Meyer– natural disasters and failure or malfunction – on the other hand, are more plausible and relevant to the Piql Preservation Services and its safety and security. Below we list the events Meyer included in the two scenario classes:[18]

Natural disaster:

- Meteorological events
    - Extreme winds (such as storms, hurricanes, tornados)
    - Extreme temperatures
    - Extreme precipitation (snow storms)
    - Flood
    - Little precipitation (such as drought, which may lead to forest fires)
- Geological events
    - Earthquake
    - Volcano eruption
    - Tsunami
    - Avalanches (such as dirt, mountain snow)
- Cosmological events
    - Meteor showers
    - Radiation (such as sun storm)

[18] We found that Meyer does not list forest fire as a relevant risk. We, however, find it relevant, and include it under meteorological events – little precipitation.

Failure/malfunction:

- Harmful emission
  - Chemical
  - Biological
  - Radioactive
- Conventional accidents
  - Explosions/fire
  - Structural collapse
  - Transport accident
- Failure of service or utility supply
  - Failure of vital infrastructure
  - Failure of vital societal functions

All of the events identified to have an impact on the security of a nation are also relevant risks to the Piql Preservation Services. Hence, they will form part of the sample space when the final selection of scenario classes is chosen and the specific scenarios descriptions are written out.

6.3.2 Applied to Issues of Security

Morphological analysis works well with events caused by intentional acts, deliberation and calculation. We have here created our own morphological box adapted to the problem in the report.

The process is separated into two phases: the analysis phase and the synthesis phase. We must begin with the first step of the analysis phase, which is to concisely define the problem. In this report a relevant question/problem would be: *What are all intentional threats and challenges that the Piql Preservation Services may face today and for 500 years to come?*

The next step is to define the parameters which best characterise the problem we have defined in the preceding step. As we focus on intentional acts, the threats would have to be directed at the Piql Preservation Services itself, apart from nuclear war and terrorism as explained previously. A logical place to start is therefore to characterise the threat actors with an interest in attacking the Piql Preservation Services, their intentions and capacities.

Hence, the following parameters were defined:
- Actor
- Goal
- Method
- Means

The next step is to assign a range of relevant values, or conditions, that each parameter might have. Here it is very important to define the values very clearly. The values should be mutually exclusive and exhaustive for the given parameter in accordance with the problem. We have made broad assumptions and cast wide nets when it comes to our parameters and definitions.

This is because one of the criterions for the parameters is that they should be exhaustive. With such a width of possible threats to so many phases of the Piql Preservation Services, it was necessary to start wide in order to narrow it down in the scenario descriptions. Also, we are using this method to arrive at risk scenarios which describe risks and threat against the Piql Preservation Services system today but also for 500 years to come. Hence, we cannot simply assume that the only methods and means that will be used are ones we know of. The values we have assigned to the parameters are all-encompassing categories, which will be described in the following. For extended definitions, see appendix A.1.

1. *Actor*: The actor parameter describes the actors who could have the intentions and capacities to pose a threat to the Piql Preservation Services. The relevant values assigned here are:
   - State
   - Network
   - Company
   - Individual

2. *Goal*: The goal parameter specifies the possible goals that a threat actor would hope to achieve, or the incentives for their actions towards the Piql Preservation Services. The relevant values assigned here are:
   - Political power
   - Market power
   - Economic gain
   - Idiosyncratic interest

3. *Method*: The method parameter describes the actions a threat actor would take to achieve their goals. The methods vary regarding how demanding they are to implement, and thus represent different levels of ambition and capacity [39 p.13]. The relevant values assigned here are:
   - Physical destruction
   - Physical manipulation
   - Logical destruction
   - Logical manipulation
   - Insider

4. *Means*: The means parameter describes the relevant resources a threat actor might employ to implement a given method, their capacities. The specific acts required of the given method are also briefly touched upon. The relevant values assigned here are:
   - Conventional weapons
   - Non-conventional weapons
   - Hand or power tools
   - Malicious transmitters
   - Software tools
   - Monetary means

The parameters and corresponding values are summarised in table 6.3 below.

Actor	Goal/purpose	Method	Means
State	Political power	Physical destruction	Conv. weapons
Network	Market power	Physical manipulation	Non-conv. weapons
Company	Economic gain	Logical destruction	Hand or power tools
Individual	Idiosyncratic interest	Logical manipulation	Malicious transmitters
		Insider	Software tools
			Monetary means

Table 6.3 Matrix for analysis of scenario classes of intentional acts

The analysis phase is now completed, and we move on to the first step of the synthesis phase. First we do a consistency analysis to narrow down the morphological space (all theoretical possibilities that exist in the matrix) to include only plausible ones. The total theoretical possibilities in the matrix here is 4 x 4 x 5 x 6 = 480 theoretically possible combinations. To reduce the complexity of trying to find consistency in all parameter values at once, we evaluate pairings of values separately and compare them one by one. We now have the solution space for the problem. The consistency matrix can be found in appendix A.2.

The next step is to feed this information into an IT tool developed for use in MA at FFI, which finds consistent parings on all four parameters, not just couples of values. We are then presented with the outcome matrix for our problem, which serves as the framework for describing concrete challenges and risks. The framework in itself is quite generic, i.e. it only includes the main factors needed to describe a completed scenario. The outcome matrix can be found in appendix A.3. Our consistency analysis produced the necessarily large number of 70 consistent solutions on all parameters, i.e. 70 scenarios. This number is perhaps abnormally large for a morphological box this size, but it was to be expected, as the broad definitions of the parameters are made to include so many features. Regardless, it necessitates a reduction by going through the scenarios in search of common denominators in order to put them into scenario classes.

Having done a qualitative evaluation of all the scenarios, we have arrived at the following scenario classes as relevant threats to the Piql Preservation Services. As with the hazards associated to issues of safety, these threats related to issues of security presented in the following will form part of the sample space when the final selection of scenario classes is chosen and the specific scenario descriptions are written out.

Crime:

- Theft
  - For profit through own usage/implementation
  - For profit through sale to third party
- Organised crime
  - For profit through own usage/implementation
  - For profit through sale to third party
- Extortion/Blackmail
  - Theft of film with sensitive information for use other than selling film directly

Sabotage:

- Of the structural integrity of the building housing the storage facility
  - Physically damaging the structure, or structural dependencies
  - Physically damaging the security barriers
- Of the piqlVault system
  - Physically damaging the components of the piqlVault system, such as the grid
  - Logically malware on the EWMS of the piqlVault system to create chaos is the system.
  - Jamming the radio signals.
  - Altering the contents of the radio signals to create chaos is the system.
- Of the Piql system production
  - Malware which alters information during preparation for printing
  - Physical damage to the piqlWriter and piqlReader
- Of the piqlFilm
  - Physically damaging the piqlFilm, perhaps by tearing it up, cutting away frames or scratching the length of it with a nail.

Espionage:

- Spyware installed in the Piql IT system
- Malicious transmitters from outside the facility

Terrorism:

- As revenge on data owner for various (perceived) offending actions
- piqlFilm as collateral damage

Armed conflict:

- piqlFilm is the target of a coordinated attack

Nuclear war:

- piqlFilm as collateral damage

6.4 Final Selection of Scenario Classes

The purpose of the scenarios chosen is to identify and analyse vulnerabilities and security challenges faced by the Piql Preservation Services today and for 500 years during production, transportation and storage. Based on the discussion above we have made the following selection of scenarios:

- **Accident**: An unfortunate incident that happens unexpectedly and unintentionally. Something that happens by chance or without apparent cause [44]. By accident we mean an event with negative consequences, be it loss of life or material damage and economic loss, which was unintended. The cause can be, but not limited to, human error.
- **Technical error**: Technical error can cause a cease of operations or functionality in a system, which here has a negative effect.
- **Natural disasters**: A sudden natural accident or catastrophe that causes great damage or loss of life.
- **Crime**: An action which constitutes a serious offence against an individual or a state and is punishable by law [44]. It can be politically motivated, economically motivated or simply due to a wish to inflict pain, perhaps due to illness.
- **Sabotage**: Intentional destruction, paralysis or shut down of equipment, materials, facilities or activities, or intentional disarmament of persons, executed by or for a foreign state, organisation or group [18 § 3,4]. Wilfully or deliberately destroy or obstruct, especially for political or military advantage [44].
- **Espionage**: The gathering of information by the use of secret and underhanded means in an intelligence capacity [18 § 3,3].
- **Terrorism**: Illegal use of, or the threat of the use of, force and violence against persons or property in an attempt to place pressure on a country’s government, population or society at large to reach political, religious or ideological goals [18 § 3,5].
- **Armed conflict**: Armed conflict is a conflict between states or groups that involves the use of armed force. This term captures better the different types of conflict that are relevant in today’s threat environment than the more traditional and more confining term “war” [45].
- **Nuclear war**: Nuclear war is a warlike state in which the main means are weapons of mass destruction.

Nine is the number of scenario classes required to map the entire spectrum of threats faced by the Piql Preservation Services. The final number of specific scenarios that will be described is even higher, partly because it is necessary to include more than one natural disaster. Describing the scenarios in detail is the final step in the morphological analysis method applied in this report. Morphological analysis is used as a tool to clarify the fundamental conditions or premises for a given scenario, and from these results we can write a detailed description of the future event [39 p.10]. As a final step we can analyse the findings in the completed scenarios, i.e. which vulnerabilities and security challenges the Piql Preservation Services is faced with in order to give recommendations of development tasks to help solve these. However, the scenario descriptions must first be written out.

The number of scenarios chosen to be part of the assessment is abnormally large for an assignment this size, yet it was unavoidable as the risks and threats which may harm the Piql Preservation Services in its current application areas are so many. Including such a large number of scenarios is made possible by the use of a scenario template. We now turn our attention to the development and adaptation of the scenario template, and finally, present the finished scenarios for further analysis.

7 Developing a Scenario Template

The purpose of developing a scenario template to help with the process of scenario description is twofold. The first is that it will enable thorough analysis of a greater number of scenarios. A risk assessment of this scale necessitates a wide range of scenarios covering a wide range of possible security challenges and vulnerabilities threatening the Piql Preservation Services. Making use of a template means that we can more easily cover a greater number of scenarios without the risk of omitting important elements as they are all clearly and distinctly laid out.

The second reason for utilising a template for the scenario description is simply ease of use for interested parties at later stages. As this report is part of a larger project, it is meant to be used by the Consortium partners in later work packages when revised design and requirement specifications of the components of the Piql Preservation Services are developed. By using a template, the format of every scenario is identical, which makes them clear and comprehensible. The vulnerabilities and the security challenges faced by the Piql Preservation Services are distinctly listed, making it easier for the Consortium partners to refer back to the scenarios and the risks they identify if needed. In the template it is also possible to list divergences from the ISO standard used as ideal storage conditions that may occur in a scenario for future testing purposes. Additionally, by presenting the scenarios in this stylised form, it is meant to be simple for existing and potential Piql partners to use this general risk assessment when analysing their own more specific safety and security needs. They should easily be able to follow the logic of the developments in the scenarios and adapt it to their circumstances, or they can even use the empty template as an initial tool to perform their individual risk and vulnerability assessments.

The scenario template used in the report to develop risk scenarios for the Piql Preservation Services is shown in figure 7.1. The text in italics is instructions and explanations on what information is to be filled in, and is meant to be replaced by the relevant information for a given scenario.

TEMPLATE FOR DEVELOPMENT OF RISK SCENARIOS IN THE NRF PROJECT “PRESERVIA”

Scenario *number*	
Scenario title	
Scenario justification	
Justification for the choice of scenario. References to past real events, if any, and the inspiration for choosing this scenario. *Purpose of the scenario, i.e. illustration of challenges/vulnerabilities needed to be dealt with in the Piql Preservation Services, etc.* *Benefit for the PreservIA project, i.e. adjustments made to piqlFilm, piqlBox, piqlVault, etc. To be used in later WPs on requirement and design specifications.*	
Scenario outline	
Short description of the context and events leading up to this scenario and the cause of the incident. *Short description of the incident, i.e. what happens, and when, how and in what environment does the incident occur.*	
Cause	
Type of risk (Hazard/Threat)	
Intentional (Yes/No/Both)	
Profile of actor (if intentional)	*Short description of profile of actor that is willing and capable to conduct event, including ‘modus operandi’.*
Description of cause	*Threat: motive, if it is an intentional act. Why is the value that the Piql Preservation Services is protecting valuable to this actor? (Intention).* *Hazard: type of hazard and brief description of properties. Cause of the accident or natural disaster, if it is an unintentional event.*
Competence and resources (if intentional)	*Applicable for intentional events: Needed level of competence and availability of resources (equipment and economical means). (Capacity).*

User/value	
User class	*Sector.*
User type	*Market area.*
Value	*What is the value to be protected? What type of information? How is it valued? Why is it valuable? Is it irreplaceable?*
Location	
Location description	*Geographical zone, with brief description of climate zone (local geographical and typological conditions), developmental level (general standard of infrastructure and work culture) and political stability (stable borders, internal threat actors). Include what is relevant for the scenario.* *City or countryside?*
Environment description	*Local weather conditions.* *Time of year (with regards to temperature, etc.)* *Time of day (with regards to personnel on duty).* *Year/Time period. The same hazard/threat can occur many times from a point onwards. If the hazard/threat presupposes a different setting in future, then the time period would simply start at a later point in the future and onwards.*
Vault description	*In mountain or in building. If in building: in basement, lower or upper floor?* *Inside environment.*
Local safety measures	*Fortified walls, seismic resistance, fire protection, water protection, radiation protection, EMP protection, utility backup.*
Local security measures	*Physical security measures on access control, camera surveillance, alarm systems and sensors, and number of personnel.*
Consequences	
Outer building	*Damages on physical infrastructure of building or mountain facility.*
Vault	*Security challenges/vulnerabilities for vault.*

Box	*Security challenges/vulnerabilities for box.*
Film	*Security challenges/vulnerabilities for film.*
Power/energy supply	*How was the power supply affected?*
Divergence from ISO standard	*Specified deviations from ISO standard in the vault concerning temperature and relative humidity, and the time duration of the divergence.*
Security mechanisms	
Integrity	*Brief summary on effects on integrity.*
Availability	*Brief summary on effects on availability.*
Confidentiality	*Brief summary on effects on confidentiality.*
Immunity	*Brief summary on effects on immunity (against attacks on CIA).*
Recommendations	
Recommended protective measures	*List the safety or security measures which could alleviate the consequences of the scenario.*
References	
Relevant literature	

Figure 7.1 The template used in the scenario descriptions

The template is based on one already developed at FFI during a previous project, but has been customised to the PreservIA project and developed further.[19] All of the factors which were presented and clarified in chapters 5 and 6 of the report – geography, timeframe, user class and corresponding asset, location and type of storage facility, and, lastly, if the scenario describes an intentional act, the threat actors and their intentions and capacities – are included in the template. By inserting the relevant information, together these factors should give a detailed description of the future event in the scenario. Furthermore, the template presents the ensuing consequences of the event and specifically how the Piql Preservation Services components and surrounding environment are affected. Finally, the effect of the event on the security properties CIA and immunity can be briefly outlined. Thus concludes the complete description of the events unfolding in the scenario and their consequences. The template then allows for a brief listing of recommendations of measures to alleviate the consequences of the event. It should be

[19] Based on the template developed in the PRACTICE project, see [46]

noted that these will be discussed more comprehensively in later sections of the report. The template finally includes the opportunity to include all relevant literature used when developing the scenario, if the need to verify the information cited should arise.

It has been decided that all information in the scenario descriptions must solely be based on open source information. This is so the final report can receive a status of unclassified and be accessible to all existing and potential Piql partners. As a result the more severe scenarios, particularly those describing intentional acts, must be kept at a generic level regarding setting and threat actor. Drawing on available statistics, historical incidents and previously published scenarios should suffice.

8 Presenting the Scenarios

In this chapter we briefly present the contents of the scenarios. We have briefly outlined the course of events, the ensuing consequences for the Piql Preservation Services and the effects on the security properties CIA. The complete details of the scenario descriptions can be found in the filled-in scenario templates which we have included in the report as appendixes.

Scenario 1 presents an accident at a nearby chemical plant caused by a human error. Chlorine gas is released into the humid atmosphere. The emissions reach the piqlVault, which has been left open by the employees during the evacuation, giving the gas unimpeded access to the vault. The piqlBox and –Film are subjected to prolonged exposure. The piqlVault system is left largely undamaged by the reactive gas, but the piqlBoxes and piqlFilm most exposed to the gas, i.e. those at the bottom of the grid, are damaged. The piqlFilms that the gas reaches are corroded, especially the gelatine emulsion where the information is written. This severely affects integrity and availability, as the data is destroyed and is thus no longer readable or accessible. However, neither is the data readable to anybody else anymore, so at least confidentiality is left intact. See appendix B.1 for full details.

Scenario 2 presents a technical error causing sparks to ignite in the electrical system which powers the piqlVault system. This error causes the system to malfunction and shut down, as the faulty wires cannot direct electricity generated by the backup generator. The sparks cause an electrical fire at the charging stations at the top of the grid which spreads. The fire sets off the sprinkler system in the building, helping to control the flames, but also dousing the piqlBoxes and –Films in water. More water is added once the fire department arrives. The piqlBoxes and PiqlFilms near the top of the grid that are touched by the flames are damaged beyond repair because they quickly start to melt. The piqlFilms doused in too much water by the fire hoses and the ones near the bottom of the grid where water starts rising may be damaged because the piqlBoxes are not water-proof. The incident does not affect the confidentiality of the information on the films, yet availability and integrity is compromised temporarily or irrevocably for the piqlFilms too badly damaged either by fire or water. Some may be saved with the proper treatment. See appendix B.2 for full details.

Scenario 3 presents a natural disaster in the form of an extreme flood during rainy season made worse by the effects of climate change. Due to the placement of the piqlVault in the basement, the raging waters quickly fill the entire space and completely submerge all the piqlFilms in the vault in extremely filthy water for days. Although the piqlVault system grid remains upright and the piqlFilms are kept in their original position inside the piqlBoxes, the boxes are not water-proof and filthy water can seep in and immerse the piqlFilms. The severity of the flood means that access to the piqlFilms is impossible for several days and they are all destroyed (we assume, but testing is necessary). The confidentiality of the information on the piqlFilms remains intact, as none with authorised access would be able to read it during the incident. Neither, however, would the data owner. Because the piqlFilms are assumed to be destroyed, the integrity of the information, as well as the availability, is compromised. See appendix B.3 for full details.

Scenario 4 presents an alternative natural disaster: a forest fire, which is also made larger and more violent by the effects of climate change. After a period of excessive heat and drought, the piqlVault, which is placed in the lower floors of a building situated in the urban/rural interface, is caught in a fierce forest fire. The local fire department are unable to get control of the fire for some time and it is allowed to rage in the vicinity for a fortnight. Not only are many of the piqlFilms and –Boxes irreparably damaged by the fire, but the data owner is also unable to gain access to the building for a very long time due to the dangers of the forest fire reaching the building again. Availability is thus compromised for all the films for a fortnight, and forever for the ones which were destroyed by the fire. The same is true for the integrity of these films, whereas confidentiality is only threatened but not compromised. However, as the piqlVault was equipped with a highly effective fire suppression mechanism, many of the piqlFilms which would have been destroyed by the fire had another fire protection measure been in place were saved. See appendix B.4 for full details.

Scenario 5 presents the final natural disaster covered in the report. An earthquake measuring 7.5 on the Richter scale hits the city where a piqlVault is located during the middle of an intense heat wave. The skyscraper, in which the piqlVault is situated in one of the top floors, remains standing, but its infrastructure is badly damaged, leaving the piqlFilms in the vault exposed to the elements and allowing warm humid air to flow freely into the vault. The water pipes around the storage room burst, soaking the piqlFilms in water, and the electrical system is also damaged, which means that the ventilation system fails. Pieces of concrete fall from the broken ceiling onto some of the piqlBoxes. The integrity and availability of the piqlFilms which are struck by the pieces of concrete is irrevocably compromised. If the piqlFilms which are exposed to the water from the ruined pipes is not dried and handled correctly, their integrity and availability may be compromised as well. For the remaining PiqlFilms, the integrity and availability may be compromised if they are left too long exposed to high levels of temperature and humidity, as this affects the readability of the information. Confidentiality is threatened, as the security parameters surrounding the piqlVault are no longer in place, but the instability of the building's structure means that no one can enter anyway. See appendix B.5 for full details.

Scenario 6 presents the theft of sensitive piqlFilms committed with the help of an insider. In a future setting where tougher market competition necessitates more brutal means of getting ahead, the oil company X bribes a high level employee with complete access to the EWMS in the piqlVault system, who manages to leave the facility with the relevant piqlFilms without being stopped. The piqlFilms contain information on a new method to do oil well analysis, which can make "dry" oil wells profitable again. Though the transaction is logged and the culprit is caught, the damage has already been done because the trade secrets, and thus also market shares, have already been lost. Although the integrity of the information was not tampered with, its availability to the data owner was compromised and, more importantly, so was its confidentiality. See appendix B.6 for full details.

Scenario 7 also presents the theft of sensitive information, though in this scenario the threat actor is an organised crime syndicate with access to heavy firepower, and the criminal act takes place while the piqlFilms are transported from the production site to the storage facility. As part of a scheme to expand their revenue, the crime network decides to accept a job from a third party to steal piqlFilms storing personal data which is to be used in large scale identity theft. Although the sensitive information is protected by additional security during transportation, it is not enough to stop a gang of four persons from robbing the truck at gun point, forcing the security personnel accompanying the piqlFilms to give them up on pain of death. The integrity of the information remains intact, but the availability to the data owner is lost. The confidentiality of the information is most definitely compromised, at the cost of all the people who now stand to have their identities misused. See appendix B.7 for full details.

Scenario 8 presents sabotage, a very relevant threat to the Piql Preservation Services. State X hackers are able to perform logical sabotage on the client information which is being prepared for printing. The hackers place malware in the system which utilises the interconnection between the Piql computer and the Piql I/O computer to create an open connection between the two. As the hackers now have free access to both computers' CPUs (Central Processing Unit) they can alter the client data undetected because they also change the corresponding check sum on both CPUs. Even though the Piql I/O computer does what it is supposed to and checks the integrity of the data against the designated checksum, it can find no faults and confirms the data ready for writing on the piqlFilm. The integrity of the information is highly compromised, as is the availability of the altered pieces of information. The confidentiality is compromised as well. See appendix B.8 for full details.

Scenario 9 presents espionage. Depending on the level of sensitivity of the information which is stored on the piqlFilm, the Piql system can be a target of espionage. This scenario underlines the risks involved when the digital data is processed during production before it is written onto the piqlFilm. Spyware is installed on this computer when the Piql system is used by the US military. The state X, as we will call them, manages to install spyware on the Piql computer system which the security measures in place are unable to detect. As a result, state X gains access to the designs of a weapon system developed by state Y, the major military power in the world. The spyware does no harm to the information: it simply copies the data that is located on the computer and sends it undetected to state X. Neither the integrity nor the availability of the information is affected, yet the confidentiality of highly sensitive information which can severely affect the relationship between two parties is lost. See appendix B.9 for full details.

Scenario 10 presents terrorism. A piqlVault is located in the same building as a major NGO advocating multiculturalism. One day, without warning, a lone right wing extremist places a car bomb in front of the building and offices of said NGO and remote detonates the bomb. The Piql system becomes collateral damage. The bomb is powerful enough to cause severe damage to the structural integrity of the building, but the building does not collapse. Additionally, though the piqlVault is placed on the ground floor, it is placed on the opposite side of the building to where the bomb is placed, meaning that the damage to the vault is not as severe as the front offices. However, the bomb was powerful enough to cause great damage to the piqlVault. The damage to the building was to such an extent that the temperature and humidity regulation in the vault can no longer be upheld and the films are exposed to the elements. The integrity of some of the films is compromised, as they were damaged by the falling infrastructure caused by the bomb. The rest of the films are damaged only insofar as the cold of the outside air has a noteworthy effect on them. Availability is likewise compromised, whereas confidentiality is only threatened but not compromised. See appendix B.10 for full details.

Scenario 11 presents armed conflict with strategic assault as part of the build-up to a larger confrontation. In a future setting where a state actor has set world domination as its goal, the threat actor executes a strategic assault on Svalbard, as it needs to remove what it believes to be intelligence about the state actor's military capacity. This is a step in a larger scheme to attack Europe, which the state actor believes it cannot do if European powers possess this information about them. Electromagnetic weapons (EMWs) and explosives are used to gain access to the storage facility, which is placed in a mountain repository. The electromagnetic pulses and controlled explosions do no harm to the piqlFilms, but they enable the unauthorised access of the state actor to the information, which is subsequently removed from the piqlVault. For a short period of time, the ideal storage conditions are not present in the piqlVault, but this is quickly rectified. The integrity of all the piqlFilms in the vault remains intact, but the availability and the confidently of the stolen piqlFilms is lost. See appendix B.11 for full details.

Scenario 12 presents nuclear war. In a future setting, the days of Mutually Assured Destruction (MAD) are back, yet the playing field is different than it was during the Cold War. There are a greater number of active nuclear powers, all with deterrence as their main policy, which means that the proliferation of nuclear weapons is higher and more areas of the world are directly exposed to the threat. Many warheads are directed at various major cities at all times. One such city is a major metropolis in the Middle East. A glitch in the launch system of a major nuclear power releases a missile on said city by mistake. Even though the piqlVault is not situated within the radius of ground zero where heavily built concrete structures are severely damaged and fatalities approach 100 %, it is still within the air blast and thermal radiation radius where most residential houses collapse and fatalities are widespread. The piqlVault with all its piqlFilms is, in other words, a casualty of war. As all the piqlFilms are annihilated in the explosion, the integrity and availability of the information is forever lost, whereas the confidentiality remains intact. See appendix B.12 for full details.

9 The Vulnerabilities and Security Challenges of the Piql Preservation Services

In this chapter we provide an overview of the vulnerabilities and security challenges to the Piql Preservation Services which were identified in the scenario descriptions. Additionally, some vulnerabilities and security challenges which were not a direct result of the scenario analysis are presented. As stressed in chapter 6, where the method for scenario selection was developed and the final selection was chosen, there are many possible scenario descriptions which would fit into a scenario class applicable to the Piql Preservation Services. We had to make a selection which would not describe all the vulnerabilities and security challenges. Some that we had to leave out have been described in other documents FFI have had access to. We therefore include them here as well, in order for this document to serve as a (as near as possible) complete and exhaustive list of the vulnerabilities and security challenges faced by the Piql Preservation Services.

Before the risks faced by the Piql Preservation Services are described, however, it must be stressed that the assessments made here are purely theoretical. They are based on the information we have received from Piql AS and other members of the PreservIA Consortium and evaluations of our own. The results have not yet been practically tested: we leave this up to other participants in the PreservIA project.

It should also be noted that the severity of the vulnerabilities of the Piql Preservation Services, and the consequences thereof, varies between and within different market areas. Especially with regards to threats related to intentional acts, the piqlFilms face a different level of risk depending on the varying degrees of sensitive information stored on them. Broadly speaking, the higher the sensitivity of the information, the higher the potential value and return for a threat actor, and thus the higher the commitment for said threat actor to somehow access or damage the information stored on the Piql Preservation Services, if that is their goal. Having the right security and safety measures in place thus becomes vital for the data owner, and their sophistication must be higher than if the piqlFilms stored less valuable information. It is important to address potential points of vulnerability in the Piql Preservation Services, as these piqlFilms will potentially be subjected to more attempts to compromise CIA – confidentiality, integrity and availability – than others. Additionally, the severity of the loss of information due to unintentional events increases the more sensitive the information stored on the piqlFilms is. Lacking protective measures would thus have far greater consequences where highly sensitive information is lost than if other less sensitive pieces of information were lost. The same logic is also applied to the recommendations we give in chapter 10 to help alleviate these points of vulnerability: If the information is more sensitive, a greater number of and a higher sophistication of measures are needed to protect it.

9.1 Vulnerabilities and Security Challenges Identified

Throughout the following presentation of the vulnerabilities and security challenges of the Piql Preservation Services, it will become evident that some of the risks are of greater importance than others to the overall safety and security of the system. Where this is the case, it is possible to indicate that a greater degree of emphasis should be placed here with regards to the tasks in later work packages of the PreservIA project related to improving various points of vulnerability. Where this emphasis is recommended, the decision is not based on the likelihood of a given event occurring, but rather on the severity of the consequences of that event for the Piql Preservation Services. It will also become apparent that some risks which initially seemed like obvious points of vulnerability in fact were only minor issues due to the sound choices already made by Piql AS regarding the implementation of the Piql Preservation Services.

We start by describing some general risks to the Piql Preservation Services as a whole, before evaluating specific vulnerabilities regarding the properties of the Piql components. Finally, threats from intentional acts are described.

9.1.1 “Out in the Open”

A general point about the vulnerability of the Piql Preservation Services is the fact that the piqlFilm is always more vulnerable when it is “out in the open”. This both alludes to the fact that the piqlFilm is most vulnerable at any time it is not in the piqlBox, as during the production when it is written and read back for verification, but also when the piqlFilm is outside a Piql-controlled environment altogether. This makes the transportation phase the most vulnerable phase of the entire service journey. This is when the Piql partner has the least control over the external influences on the piqlFilm, much less than during the production phase and certainly less than during the storage phase. During the two latter, the Piql partner can create a protected environment where measures and routines are in place to make sure that the piqlFilms are as safe and secure as they can be. During the transportation phase, the measures put in place are fewer and factors outside of the Piql partner control are more numerous. The dangers involved here were illustrated by the scenario describing a successful attack on a transportation truck, despite the presence of many sound security measures.

9.1.2 Inside Threat

One of biggest security challenges to the Piql Preservation Services identified is the inside threat, or “the insider”. Also known as the unfaithful servant, it involves a trusted employee or someone otherwise connected to the Piql Preservation Services. Such employees are normally properly vetted and evaluated before being trusted with their tasks, and as such they often have regular access to the Piql Preservation Services. Such an insider can act of their own volition, motivated for instance by the prospect of revenge, or they can act on behalf of someone else, possibly if they have received financial compensation for them betraying their employer, i.e. a bribe. The insider can also be forced to somehow harm the Piql Preservation Services, for example if they are the subject of extortion.

The inside threat is deemed one of the biggest security challenges to the Piql Preservation Services because it has the potential to harm all three of the security properties CIA and because the risk is present during all three phases of the service journey. The insider is, firstly, in a position to damage the piqlFilm, maybe beyond repair, affecting the integrity of the information and possibly its availability to the data owner. This can take place during production before the finished piqlFilm is sent for transportation to the piqlVault; during transportation if for instance one of the guards protecting the film during the transport is an unfaithful servant; or during storage while the physical piqlFilms are vulnerable to anyone with access to the piqlVault. However, Piql AS has made damaging the information in its physical form very difficult during production, as the design of the piqlWriter is such that the cover must be down during writing, which makes it impossible to for instance scratch the piqlFilm with a needle as it is being written.

The insider can, secondly, simply remove the piqlFilm without authorisation or facilitate others so that they can remove it, without intending to damage it. If that is the case, the availability of the information is most certainly affected and potentially its confidentiality if the unfaithful servant has the intention of sharing the information with someone. During storage, for instance, anyone with the proper access to the piqlVault system can order a pick-up of a piqlFilm and simply walk out.

Lastly, the rightly placed insider is also able to extract vital pieces of information from the piqlFilm without authorisation with the intention of sharing it with a third party, which compromises the confidentiality of the information. For instance, they can steal the original file of the client by making a copy onto a memory stick during the early phases of production.

During the storage phase, however, the threats posed by the actions of the insider are somewhat mitigated. In choosing an automated storage and handling system as opposed to a manual one, accessing the piqlFilms is not as easy as it would have been if they were stored on shelves. Picking one off of a shelf to damage it or remove it from the facility would be easy work, and the record of such an act would be non-existent. Conversely, in the piqlVault system the piqlFilms are offered some measure of protection simply by virtue of being stored in the aluminium grid which cannot be accessed without machines. Removing a piqlFilm from “the shelf” is thus no simple matter. The pick-up must be ordered electronically, which would also leave a record of the transaction, making it easier to trace later on if there is suspicion of foul play. This was the case in the scenario regarding theft of trade secrets with the help of an insider.

9.1.3 Loss of Ideal Storage Conditions

Though the use of photosensitive film as a storage technology is a proven solution which is both robust and durable, the risk of loss of ideal storage conditions must be taken into account in this risk assessment. Loss of ideal storage conditions can be caused either by loss of utilities causing the ventilation system to stop functioning, or by damages to the infrastructure of the building which houses the Piql Preservation Services causing outside air to flow into the storage facility. Unfortunately, at lot of the measures a Piql partner could conceivably put in place to ensure that the ideal storage conditions are upheld are out of their hands. All piqlVaults are placed in standard office or industrial buildings, which means that the Piql partner will have had no say in the construction of the building. They must simply trust that regulations, codes, standards and best practices have been followed during construction so that the building is best able to resist natural hazards occurring in its geographical zone. Energy supply in particular is vital to ensure the successful implementation of the Piql Preservation Services, and as such is one of the most pressing structural dependencies of the storage facility. Piql AS stipulates that all piqlVaults must have a power generator in case of a power outage, but other than this small measure the Piql partners are vulnerable to the decisions of others and how they in turn decide to implement those decisions.

In order for the 500 year longevity to be guaranteed, the storage conditions must be kept within the ISO standard regulations of no higher temperature than 21° Celsius and no higher humidity level than 50 %. If these conditions are not met, at best the result will be reduced longevity of the piqlFilms, at worst the result could be (severe) damage to the piqlFilms and the loss of the information stored on them. FFI has done calculations regarding the temperature change in the storage room should the environmental control systems fail. Due to insufficient information on the exact amount of electrical power needed in the storage room (including energy sources like lighting and data equipment) and differences in external heating in the different geographical zones, it is impossible to say anything definitive about the temperature increase in the storage room when no regulating measures are functioning. However, based on the information we have received, we assume that the temperature in the storage room will increase between 0.02 and 0.1° Celsius an hour without proper environmental controls to ensure the 21° Celsius and 50 % relative humidity as stipulated by the ISO standard. For full calculations, see appendix C.1.

The effects of increases and decreases in temperature on the piqlFilms were described in several scenarios, including earthquake, as this incident took place during a heat wave, terrorism and armed conflict. In the former the piqlBox and –Film are exposed to excessive heat and humidity, whereas in the two latter they are exposed to colder temperatures than are ideal. Also in the scenarios illustrating the effects of fire, the piqlFilms are exposed to a general increase in heat from the proximity to the fire.

The ideal storage conditions of the piqlBox are low temperatures, low levels of humidity, no ozone and limited direct light.[20] The same conditions apply for the piqlFilm. This means that,

[20] The properties and qualities of the piqlBox and piqlFilm were discussed in a telephone meeting with Espen Ommundsen, Principal Researcher at Norner AS, and Yvonne Hed, Researcher at Norner AS, on 17.09.15.

unless the temperature and relative humidity level get too low, higher levels than normal will cause more damage than lower levels. If, however, they do get too low, this may cause some changes to the mechanical properties of the piqlBox and the piqlFilm. The polypropylene (PP) of the piqlBox is not notably vulnerable to changes in humidity, but lower temperatures will cause brittleness in the material.[21] The polyethylene terephthalate (PET) of the piqlFilm, on the other hand, is affected by both lower temperatures and relative humidity. It will also cause brittleness to the point where the material might break, much like a cold rubber band.[22] In addition, lower levels of humidity may cause static on the piqlFilm due to a slight contraction of the emulsion layer where the information is written, which might cause difficulty in focusing the images in the piqlReader [27]. Fortunately, these effects can be avoided simply by conditioning the piqlFilm properly, i.e. letting it thaw under controlled conditions, before it can be handled. Piql AS has conducted extensive tests to this effect. PiqlFilms have been stored in a Cryotank which holds liquid nitrogen with a temperature of -196°C and varying levels of relative humidity for 24 hours before being defrosted under controlled conditions. When the piqlFilms were read back there were little signs of damage to neither the piqlFilm nor the data written on it.[23] Lower rather than higher temperatures and levels of relative humidity can also have positive effects on the longevity of the piqlFilm or the piqlBox. Market "best practices" when it comes to storing photosensitive films is in fact to keep the storage conditions very cold, near freezing.

Higher temperatures and relative humidity can affect the security properties of the piqlFilm in a negative manner, yet the increased levels required for the negative effects to occur are quite high. The piqlFilm has been subjected to extensive testing to determine these adverse effects. High temperatures and high levels of humidity can cause the piqlFilm to warp because of shrinkage along the edges, and it may affect readability, in the sense that the information gets blurred when the emulsion layer starts floating out [27]. The integrity of the piqlFilm would thus be greatly compromised, as the data is lost and cannot be read again. Additionally, in an environment with higher levels of relative humidity there is a possibility of growth of microscopic blemishes on the piqlFilm due to oxidation of the silver halide. Fungi may also start to grow on the piqlFilm [27]. However, the tests conducted by Piql AS in collaboration with other Consortium partners show that the temperatures required to generate these effects are very high. The piqlFilm can withstand temperatures up to 85° Celsius at a relative humidity of 50 % percent for 23 weeks before there is a loss of mechanical properties which affects the readability of the piqlFilm.[24]

There are few plausible scenarios where such conditions exist over such a long period of time. Additionally, our calculations show that the increase in temperature and relative humidity when the environmental control systems are not functioning is modest, from 0.02 to 0.1° Celsius an

[21] The properties and qualities of the piqlBox and piqlFilm were discussed in a telephone meeting with Espen Ommundsen, Principal Researcher at Norner AS, and Yvonne Hed, Researcher at Norner AS, on 17.09.15.
[22] *Ibid*.
[23] The information regarding the Kryolang project was part of an email correspondence with Janita Flo, Lab Manager at Piql AS, on 04.05.16.
[24] The information regarding the test results of the piqlFilm's exposure to high temperatures over extended periods of time was part of an email correspondence with Svein Jamtvedt, Principal Researcher at Norner AS, on 27.05.16.

hour, implying that this may not be a major threat to the integrity of the piqlFilm. However, as mentioned, these calculations do not take into account the effects of external heating, which are significant in some parts of the world, so one must assume that the unfavourable conditions will be worse here, especially if the infrastructure of the storage room is not intact anymore. Regardless, the piqlFilm is, as demonstrated, proven to withstand exposure to high temperatures over an extended period of time.

Finally, it must be noted that long exposure to imperfect storage conditions has worse effects than short exposure.[25] The materials used in the Piql components are supposed to withstand quite a lot when it comes to changes in temperature and relative humidity when it is a matter of shorter exposure. It is primarily when long-term exposure is a fact that the problems described above arise. At temperatures below 40° Celsius the piqlBox and piqlFilm will last for at least more than 50 years even if the relative humidity should increase to above 50 %.[26]

9.1.4 Fire

Fire is a major risk to the integrity of the piqlFilms, the destructive effects of which were described in the scenario where a technical error caused an electrical fire in the piqlVault system; where a forest fire raged and was sustained for a longer period of time with little opportunity to extinguish it; and where a nuclear detonation caused a mass fire devouring all in its path. Fire could also occur in the scenarios involving explosives, such as armed conflict and terrorism, but in the cases described in the appendixes, the resulting fire did not reach the piqlVault.

In a regular room fire, flame temperatures can reach between 600 and 1200° Celsius, but of course wide spatial variations will be seen. Some of the piqlBoxes and –Films will thus be devoured by the flames, whereas others will simply be exposed to excessive heat.

The same can be said for the piqlVault gird: as aluminium has a melting point of between 600 and 660° Celsius, parts of it will melt, though not burn. Yet the integrity and stability of its mechanical properties is affected at even at 200° Celsius, meaning that if the structure is still standing, it will be much weakened [47]. All operations in the piqlVault cease, naturally, making recovery of the piqlFilms difficult. Most likely, manual recovery will be necessary. Piql AS has created a solution which allows for this, but it is a complex and time-consuming process [29]. The negative effects of the fire on the piqlVault grid itself thus have an impact on the availability of the piqlFilms that are not destroyed by the flames or otherwise damaged by potential contact with the melting aluminium.

If the piqlBoxes come in contact with the fire, they too burn and melt, as they are not fire resistant. The PP in the piqlBoxes melts at 170° Celsius, and the once hard plastic will turn into

[25] The properties and qualities of the piqlBox and piqlFilm were discussed in a telephone meeting with Espen Ommundsen, Principal Researcher at Norner AS, and Yvonne Hed, Researcher at Norner AS, on 17.09.15.

[26] The information regarding the longevity of the piqlBox and piqlFilm was part of an email correspondence with Svein Jamtvedt, Principal Researcher at Norner AS, on 27.05.16.

a thick, sticky mass.[27] When the melting PP comes in contact with the contents of the piqlBox – the piqlFilm – it will compromise the integrity of the piqlFilm.

For the piqlFilms which are touched by the flames, this does not matter, as the flames most likely will cause more problems than melting PP. Though the piqlFilms' polyester base is slow-burning with enhanced resistance to heat and it is proven to withstand 121° Celsius for 24 hours without significant loss in readability or printability, it cannot withstand flame temperatures [27]. The integrity, and thus the availability, of the piqlFilms which are outside of the flames' reach, however, stands a very good chance of remaining intact. The integrity and availability of the ones which the flames do reach is compromised. The PET in the piqlFilms has a melting temperature at approximately 260^{o} Celsius, but already at a temperature of 75° Celsius the properties of the PET will change a lot. What happens is the same as when glass is heated; it will get softer and more viscous.[28]

With regards to the adverse effects of smoke on the piqlBox and –Film there is little information available. As far as FFI is aware, no testing has been done to this effect, and we do not know how the Piql components will react to smoke. It is said that smoke will have little impact on the piqlBox, but we do not know how the gelatine in the emulsion of the piqlFilm will hold up against potentially harmful toxic smoke.[29]

9.1.5 Water

Water is another major risk that could threaten the Piql Preservation Services, perhaps even more so than fire, as a fire can be somewhat controlled: water would reach and thus affect more of the piqlFilms. However, as with the issue of smoke, as far as FFI is aware, there has not been conducted any proper testing on the effects of water on the piqlFilms. The only information we have regarding the piqlFilm's reaction to water is this: "The piqlFilm's data can be unaffected by water only if the piqlFilm is immediately rewashed and dried properly, in which case the data will be readable" [27 p.3]. It goes on to relay what will happen if the piqlFilm is left to dry naturally: the layers of the coiled film reel will stick together. It says nothing about how long the piqlFilms can be submerged before other problems arise; what those problems might be; or how the piqlFilm reacts differently to clean and dirty water, which we must assume it does. Precisely these contingencies were presented in the scenario describing an electrical fire cause sprinklers to be activated and in the scenario describing a flood, where the piqlFilms are exposed to prolonged submersion in very filthy water.

Though we have no tests specifically for the piqlFilms to base our statements on, and much of the following must then be assumptions, we do have the valuable input of the Consortium partners stating that both the PP of the piqlBox and the PET of the piqlFilm is very water resistant, though the box is more so than the film. Both plastics can be submerged in water for a

[27] The properties and qualities of the piqlBox and piqlFilm were discussed in a telephone meeting with Espen Ommundsen, Principal Researcher at Norner AS, and Yvonne Hed, Researcher at Norner AS, on 17.09.15.

[28] The properties and qualities of the piqlBox and piqlFilm were discussed in a telephone meeting with Espen Ommundsen, Principal Researcher at Norner AS, and Yvonne Hed, Researcher at Norner AS, on 17.09.15.

[29] *Ibid.*

very long time without showing notable changes in their mechanical properties.[30] This makes no mention of the quality of the water, however, and we must assume that the filthy water the piqlBoxes is exposed during the scenario regarding a flood, where the water is mixed with mud, vegetation and rocks, debris and remnants of buildings, and also possibly human bodies, at the very least necessitates their replacement, as their longevity can no longer be guaranteed.

Though the plastic in the piqlBox is water resistant, that does not make the piqlBox water-proof. They are only splash-proof, which should protect the piqlFilms inside from exposure to much of the water from a sprinkler system, but as the piqlBox is not air-tight, water may find its way into the piqlBox and come in contact with the piqlFilm. If the piqlBoxes are submerged in water, this will most certainly be the case. In situations like these, we can assume that the gelatine emulsion, and not the PET base, of the piqlFilm is the weakest link. Shorter periods in colder water should cause little damage to the information on the piqlFilm, especially if they are immediately rewashed and dried properly.[31] If not, the integrity of the information may be compromised and the availability of the information is lost. When the piqlFilms are exposed to water that is acidic or basic (alkaline), or of a higher temperature, as may be the case during a flood, the resulting effects are quite different. We can safely assume that neither the polyester nor the gelatine emulsion of the piqlFilm will hold up long under these conditions. The gelatine would likely dissolve, and the piqlFilms would be damaged beyond repair. It would no longer be possible to verify the integrity of the information, and its availability would be lost.

We conclude this discussion of the effects of water on the Piql Preservation Services with one final note, though it may be obvious: The water would have a very negative effect on the piqlVault system. As an automated system, whose operations entirely consist of electronics, water is very damaging. Exposure to water causes the electronics of the system to short-circuit and the operations of the system to shut down. As mentioned previously, manual recovery of the piqlBin would then be necessary, compromising the availability of the piqlFilms for quite some time.

9.1.6 Physical Pressure from Overhead Weight

An additional risk faced by the Piql Preservation Services where there is need for testing before we can say anything definitive on the subject is the issue of how the piqlBox and piqlFilm can withstand different degrees of physical pressure from an overhead load before the piqlFilm is damaged beyond repair. In our scenario descriptions of an earthquake and a terrorist act where a bomb damages the building which houses the piqlVault, slabs of concrete either fall onto the grid of the piqlVault system or are propelled against it. Naturally, the piqlBoxes and –Films hit directly by bigger pieces of concrete are crushed. Yet the question remains how the piqlBoxes and –Films trapped beneath smaller pieces of concrete fare. These pieces would not initially

[30] The assertion that the piqlBox and piqlFilm can be subjected to water without causing much damage was part of an email correspondence with Harry Øysæd, Senior Researcher at Norner AS, on 21.01.16, where he quoted “Chemical Resistance, Volume 1 – Thermoplastics”, PDL (Plastic Design Library) Handbook Series, second edition, 1996.

[31] The assertion that the piqlBox and piqlFilm can be subjected to water without causing much damage was part of an email correspondence with Harry Øysæd, Senior Researcher at Norner AS, on 21.01.16.

crush everything they land on, but simply add more weight to the piqlBoxes and –Films underneath them.

For the piqlFilms, we have no information regarding its ability to withstand any kind of physical pressure, nor have we been informed of a standard they should adhere to on this point. All we can assume is that there is an advantage in the way the piqlFilms are tightly rolled into a coil. This way they are able to withstand more pressure than when uncoiled. The piqlBoxes, on the other hand, we know are intended to protect its contents from an impact of 5 Joule, though, no tests have been conducted to this effect.[32] An impact of 5 Joule is also quite modest, so it is unlikely that the piqlBoxes would endure the kind of pressure described in the scenarios.

9.1.7 Jolts and Drops

Initially, the issue of jolts and drops seemed to be a major problem for the Piql Preservation Services. The piqlBoxes could drop to the floor, either due to human error or external force (such as an earthquake), and the piqlFilms could fall out of the box and be damaged as a result. There is a drop test specified by the Library of Congress in the US stipulating that a container must be able to be dropped on its edge from a height of 180 cm while containing a full roll.[33] The piqlBox fails this test today, meaning that the box pops open upon impact and the piqlFilm falls out. The PreservIA Consortium has set a new requirement of 120 cm, but testing still remains, so this could potentially be an issue for the integrity of the piqlFilm.

However, the choice of an automated storage and handling system as opposed to a manual one seems to make a substantial difference on this outcome. While keeping in mind that FFI has not done any tests on this system, nor gained access to any such tests from Element Logic, meaning that this is a theoretical assessment, the design of the piqlVault system grid seems quite stable in and of itself and cannot easily be tilted or overturned. This stability is strengthened by the tight stacking of the piqlBins within the grid. The risk of upsetting the contents of the piqlBins thus seems lower than if they were stacked on shelves and manoeuvred by trollies. Additionally, minimal handling of the piqlBoxes by human operators in an automated system decreases the risk of human error, e.g. dropping the piqlBin- or Box on the floor. Though still present with an automated system, due to the human involvement during pick up and insertion into the grid upon arrival of the piqlBoxes, the risks are greater with a manual system, as the piqlFilms are exposed to these potentially dangerous situations more often.

9.1.8 Chemical Compounds

In the scenario describing the effects an accident can have on the Piql Preservation Services, we chose to examine the effects a chemical agent would have on the system if there is a leak at a

[32] The information regarding the level of external impact the piqlBox should withstand was given during a meeting with Alfredo Trujillo, Product Manager at Piql AS, and Tore Magne Skar, Project Manager at Piql AS, on 23.11.15. They were quoting Spec. Ref. IK08 in EN 62262/ IEC 62262:2002

[33] The information regarding the drop test was given during a meeting with Alfredo Trujillo, Product Manager at Piql AS, and Tore Magne Skar, Project Manager at Piql AS, on 23.11.15. They were quoting Spec. Ref. «Library of Congress Preservation Directorate Specification Number 800-852 – 11”

nearby chemical plant. We chose chlorine gas as the culprit. Yet, our understanding is that the piqlBox and piqlFilm would react similarly to a variety of chemical agents, so the effects are transferrable.

The piqlBox is somewhat chemically inert, i.e. non-active. The PP of the piqlBox is normally chemically resistant at ambient room temperatures, and most chemical compounds will have little immediate effect on the box. Problems may arise later in the form of reduced longevity. Acids and bases have no or only minor effects on the piqlBox, but strong oxidative chemicals, for instance ozone, will oxidise the material and lead to reduced longevity.[34] Specifically with regards to chlorine gas, the reactive gas can make the chemical bonds in the PP break and cause the material to crack. However, for the negative effects of chlorine gas to become evident, higher temperatures and more humidity in the air are required. At 20° Celsius and normal levels of humidity, the damage is almost non-existent. We need temperatures of 60° Celsius and large amounts of water in the air to be able to see severe damage [48].

Contrary to the piqlBox, the piqlFilm is very susceptible to the negative effects of chemical gases. As the piqlBox is not air-tight, the gas will come in contact with the piqlFilm. The PET of the piqlFilm, as a polyester, is degraded by very strong acids and bases, especially when exposed to the compounds for longer periods of time in higher temperatures. When the compounds are mixed with water, the effects are worsened.[35] For instance, the PET is resistant to chlorine gas which is dry at 15° Celsius, but not resistant at 66° Celsius. When the gas is wet, however, the PET is not resistant at either temperature. That means that a sufficient level of humidity in the air can make the chlorine gas cause severe damage to the base of the piqlFilm [49]. As with the risks presented by exposure to water, however, it is the gelatine in the emulsion layer which is the weakest link. Because it is a protein, it will dissolve completely at very little exposure and will react violently with corrosive gases such as chlorine gas.[36]

9.1.9 Harmful Microorganisms

We did not include a scenario which describes how the Piql Preservation Services reacts to harmful microorganisms in our scenario analysis. However, we thought it important to include, especially as the properties and thus reactions of the piqlBox and piqlFilm are quite similar when exposed to both chemical agents and biological agents. The piqlBox is biologically inert, i.e. biological compounds have little or no influence on the piqlBox. The piqlFilm, however, cannot be described as being biologically inert. The PET of the film is resistant, but the gelatine in the emulsion on the piqlFilm, as a protein, is very biodegradable. Though the presence of silver, which is an effective biocide, in the photosensitive emulsion could protect the gelatine, gelatine is known to be degraded by fungi, bacteria and other microorganisms and dissolves at exposure to harmful microorganisms.[37]

[34] The properties and qualities of the piqlBox and piqlFilm were discussed in a telephone meeting with Espen Ommundsen, Principal Researcher at Norner AS, and Yvonne Hed, Researcher at Norner AS, on 17.09.15.
[35]The properties and qualities of the piqlBox and piqlFilm were discussed in a telephone meeting with Espen Ommundsen, Principal Researcher at Norner AS, and Yvonne Hed, Researcher at Norner AS, on 17.09.15.
[36] *Ibid*.
[37] *Ibid*. Additional information from email correspondence with Svein Jamtvedt, Principal Researcher at Norner AS, on 27.05.16.

9.1.10 Nuclear Radiation

We now move our attention over to the risks presented by different types of radiation: nuclear, electromagnetic and ultraviolet radiation. In the scenario describing the consequences of a nuclear detonation, we briefly touched upon the effects of nuclear high-energy radiation on the piqlFilm. The scenario was included to illustrate the vulnerability of the Piql Preservation Services to its surroundings, emphasising that in such a scenario, there is little the Piql partner can do: As the piqlVault is stored within the air blast and thermal radiation radius of ground zero, the Piql Preservation Services is annihilated along with everything else [50]. Such a scenario illustrates the uncertain future of the system, as we have to think 500 years ahead. Still, we thought it sensible to also image a slightly different scenario: one, in which the piqlFilms are located just outside of the thermal radiation radius, i.e. just out of reach of the destruction caused by the detonation but instead exposed to the maximum amount of radiation from the radioactive fallout. In this setting, the piqlFilms would suffer exposure to high-energy radioactive fallout over a long period of time.

The plastic materials in both the piqlBox and the piqlFilms are affected by this exposure to radiation, but not to the extent one might expect. The PET of the piqlFilm will harden and develop small cracks under irradiation, but the effects are barely significant. The PET is less sensitive than the PP of the piqlBox, which will become brittle and lose all of its elongation and almost all of its tensile strength due to the high-energy nuclear radiation, necessitating their replacement [51]. Neither is the gelatine in the emulsion layer affected as negatively as one might imagine. As a protein, it would require quite high dosages of the ionising radiation to cause visible or notable radiation damage to the gelatine [52, 53]. In fact, it would seem that the gelatine could survive such high levels of radiation that, if ionising radiation was the only threat this close to the ground zero, it would survive just outside the radius where the initial radiation is at its highest after the detonation. However, that is obviously not the case. Even if the data is not lost due to the high levels of radiation, it would still be destroyed by either the air pressure from the initial blast, the heat wave or the ensuing fire caused by the firestorm which could burn the building housing the piqlVault to the ground. Outside of the thermal radiation radius, however, where the piqlFilm is merely exposed to radioactive fallout, the radiation levels are not high enough to have a noteworthy effect on the emulsion layer [54]. The piqlFilm should, in other words, survive a nuclear detonation if the distance to ground zero is such that the air blast and firestorm does not destroy it.

9.1.11 Electromagnetic Radiation

Electromagnetic radiation, or electromagnetic pulses (EMP), on the other hand, will have no influence on the piqlBox or piqlFilm. In a weaponised form, EMP can be referred to as High Power Microwave (HPM), which emits at short bur of high intensity energy [55]. This can disable or destroy electrical equipment, but it will have no effects on plastics. The piqlBox and the information of the piqlFilm are, in other words, safe from harm, but the piqlVault and piqlVault system fare worse. Electronic security measures present in and around the piqlVault will be affected. Documented effects include alarms being deactivated, electronic locks being opened and surveillance systems failing. In addition, all operations of the piqlVault system, as an automated system, will cease. The robots in particular can be damaged if there is an overload on several of its finer electronic components at the same time. The electromagnetic pulses will also destroy the data which is transferred via the radio signals from the Controller to the robots, impeding the movements of the robots [55]. The availability of the piqlFilms may then for a time be compromised as repairs to the electronics of the piqlVault system must be undertaken before the system can operate fully again.

9.1.12 Ultraviolet Radiation

The final type of radiation covered here is ultraviolet (UV) radiation. The risks to the Piql Preservation Services connected with UV radiation were not included in a scenario, but we thought it worth mentioning, as its effects of the piqlFilm are important to be aware of. The mechanical properties of PET of the piqlFilm will be somewhat degraded by UV radiation, as all plastics are, though it will hold up better than the PP of the piqlBox.

Most harmful, however, are the effects on the emulsion layer on the piqlFilm. The silver halides contained within it are photoactive, as this is how the information is written onto the piqlFilm. This means that they will be bleached if left out in sunlight or UV radiation from lighting in the ceiling. Under normal storage conditions the piqlFilm is coiled and placed in a piqlBox, and these packaging features both should protect the piqlFilm from exposure to UV radiation. Yet, it is possible to imagine scenarios where the piqlFilm can be exposed to these adverse conditions, for instance if it is thrown from the building on a sunny day during production due to an explosion. Should a similar event occur, and the piqlFilm is bleached in this way, it cannot be read back and the information is lost.[38] This is also why adhering to the production and storage conditions concerning lighting is so important.

We have now described some risks related specifically to the properties of the Piql components. We now turn to threats which would not be present but for the malicious intent and actions of others. As such, we will more thoroughly describe the challenges faced by the security parameters surrounding the Piql Preservation Services.

9.1.13 Theft

As a storage medium of potentially very valuable and sensitive information, the Piql Preservation Services can likely be the victim of theft throughout its existence. Theft is one of the biggest threats to the Piql Preservation Services, as well as one of the more consistent ones, as we can safely assume this risk will be present throughout the 500 years included in this risk assessment. So long as the piqlFilms store information which is of interest to someone else, that threat actor may attempt to steal it, which would greatly compromise the availability and confidentiality of the information. The motivation for the theft can be either making a profit through the own usage and implementation of the information stored, or by selling it to a third party. A third option is to use possibly sensitive information about an individual or organisation

[38] The properties and qualities of the piqlBox and piqlFilm were discussed in a telephone meeting with Espen Ommundsen, Principal Researcher at Norner AS, and Yvonne Hed, Researcher at Norner AS, on 17.09.15.

as extortion and force them to act a certain way which is beneficial to the threat actor. The threat actor can either be working alone or it can be an organised effort, where the piqlFilm is the target of organised crime. Perhaps the largest concern, as mentioned previously in this chapter, is that the theft can be executed with the help of an insider.

There is an important distinction to be made with regards to theft of the information stored with the Piql Preservation Services between physical and logical theft: by logical theft we mean stealing the information while it is stored or transferred electronically; [39] and by physical theft we mean stealing the physical storage medium, i.e. piqlFilm, which stores the digital data.

As the Piql Preservation Services is mainly an offline storage medium, there is limited opportunity for a threat actor to attempt to steal the information stored on the piqlFilm by logical means. This is only possible when the information is in contact with online networks, i.e. during the production phase. [40] The Piql technology is true WORM – Write Once, Read Many – and once it is written, it cannot be modified. Because there is less need for migration of the data than with other storage media due to this feature, there is also less need for contact with online networks. Fewer parties are involved with managing the information as well, as there is less need for maintenance. The opportunities for logical theft are thus fewer, and the risk thereof decreases as a result. Nevertheless, a threat actor could gain access to the data during the production phase, which we will elaborate on in the section below regarding computer security.

If a threat actor wishes to steal information stored on the piqlFilm at any other point in the service journey, this must involve the physical removal of the piqlFilm. As mentioned earlier in the analysis, this risk is greatest during transportation, when security is at a minimum because the piqlFilms are not in a Piql-controlled environment. The risk of physical theft is also very much present during storage, however, as it is possible for someone to gain access to the storage facility despite the presence of security measures. This can be done by force or by cunning. Once again, though, the choice of an automated storage system can serve to mitigate certain risks, here the ease with which theft is possible. In a manual system, the threat actor needs only gain access to the storage room, grab the correct piqlBox and run. With the automated system, however, an outsider would have more difficulty in, first, gaining access to the piqlVault system, and, second, understanding how to work the system. This would require additional planning and intelligence gathering beforehand, which might be enough to deter a threat actor from acting. They can, unfortunately, instead enlist the help of an insider, which, as mentioned, is a big concern. In doing so, they bypass the problem of not having intimate knowledge of the system altogether.

9.1.14 Sabotage

Sabotage of the Piql Preservation Services is also a major concern, as there are so many components of the system that can be tampered with. Especially when one considers that the

[39] By logical threats or hazards we mean risks against the Piql Preservation Services while the information is stored or transferred electronically. See [56, p.18].

[40] The reader will remember that some of the information stored on the piqlFilm will also be connected to online networks during data retrieval, but this step in not directly included in this assessment.

motive of the threat actor might not be purely to damage the information stored itself, which compromises its integrity, but simply create chaos and thus affect availability, the negative consequences of sabotage increase. Sabotage can primarily take place in two phases: during the production phase and the storage face. The target of the sabotage can be the building which houses both the production site and the storage facility; it can be the necessary machines in the production process, i.e. the piqlWriter, piqlReader and the equipment used when developing the piqlFilm. It can be the piqlVault system grid and the corresponding machinery; and the target can of course be the piqlFilm itself. As with theft, there is a distinction between logical and physical sabotage, i.e. somehow damaging or altering the information while it is being stored or transferred electronically, or somehow damaging the physical entities and surroundings of the Piql Preservation Services.

We will now list the identified possibilities for both physical and logical sabotage during both the storage and production phase.

During the storage phase, the main risks of sabotage are of a physical nature. There is only one real logical threat to the operations of the automated storage system, i.e. the piqlVault system, and that falls under sabotage. Logical theft or espionage is not a real concern, as there is no logical information stored in the piqlVault system which is of interest to a threat actor. Only the unique reel IDs of the piqlFilms and the corresponding local IDs which are used to specify their location in the piqlVault system is stored electronically: should you want to access any valuable information during the storage phase, you would need to get your hands on the physical piqlFilm, i.e. steal it, which has already been covered. It is, however, possible to affect the availability of the piqlFilms by logically sabotaging signals which are transferred in the piqlVault system and essentially wreaking havoc inside the grid. A threat actor could gain access through the potentially vulnerable interface network between the Piql IT system and the piqlVault IT system (the vulnerability of which is expanded on below) and install malware in the EWMS which switches the reel IDs around or orders random pick-up continuously. A second option is if a threat actor somehow manages to affect the radio signals controlling the movements of the robots through the use of a malicious transmitter, either jamming the signals completely and halting all operations, or if they are able to break through the security protocol protecting the radio signals to alter their contents and sending the robots all over the place in the grid. Again, this would have no effect on integrity or confidentiality, but the availability of the piqlFilm would be compromised.

Though the possibilities of logical sabotage are limited during storage, the opposite is the case for physical storage. Here, sabotage of the building housing the storage facility is possible, like blasting a wall; its structural dependencies such as energy supply can be tampered with if someone for instance cuts some vital cables; and its security barriers can be affected by taking a sledgehammer to important control systems. The grid of the piqlVault system can also be physically damaged, for instance if someone drives a truck right into it. Depending on the severity of the sabotage, the integrity of the information on the piqlFilms may be affected, but there is no question that availability is affected.

During the production phase, the severity of the sabotage on CIA is greater with logical sabotage than with physical sabotage. Physical sabotage primarily includes inflicting damage to the machines necessary in the production process, which does little to the Piql Preservation Services other than to delay production, whereas logical sabotage can do some real damage. We will elaborate on how this is possible in the section below regarding computer security, but if the threat actor possesses enough skill, they can gain access to the Piql IT system and make alterations to it which makes it unable to detect whether files have been altered during the process of preparing the data for writing. In this scenario, entire files of information or just parts of the files can be damaged beyond repair or deleted altogether, severely affecting the integrity of the information.

Finally, the piqlFilm itself in its physical form can be damaged as a result of sabotage, and this can happen during all three phases of the service journey, at any point after the piqlFilm is written. An insider or someone else who gains access to the piqlFilms unnoticed can tamper with the film. The sabotage can be subtle, like cutting away a few important frames and meticulously patching the film back together, or more crude like scratching the length of the piqlFilm with a nail. Either way, the information is altered and the integrity lost. As with theft, sabotage can also be done with the help of an insider, which increases the risk. An insider can even decide to cause the damage themselves, for instance if they feel they have been poorly treated and are seeking revenge.

As demonstrated, sabotage is a real concern of the Piql Preservation Services, simply due to the sheer number of ways a threat actor can negatively affect the various components of the system. Although some acts of sabotage will have less negative consequence on the most important feature of the system, i.e. the information on the piqlFilm, they would still do damage to the system as a whole, affecting its functionality and therefore also the availability of the information. The Piql Preservation Services is an intricate service, and damaging one element will have consequences for the whole.

9.1.15 Espionage

When the sensitivity of the information stored on the piqlFilms is such that it is sufficiently valuable to a threat actor, the risk of espionage is present. Espionage involves tasks which can be undertaken by individuals, companies and, of course, states. We have previously defined espionage as the gathering of information by the use of secret and underhanded means in an intelligence capacity. Such gathering of information would, of course, include secretly getting a hold of the physical information of the piqlFilm, but we have put this action under theft in this assessment. Espionage and intelligence gathering comes in many forms, but of particular interest here is signals intelligence, or information gathered from the interception of signals [30]. In other words, we view it primarily as a logical risk to the Piql Preservation Services. This, in turn, means that it would only happen during the production phase, as this is the time when the valuable information is connected to online networks. As mentioned, there is no valuable information to spy on in the piqlVault IT system.

Unlike sabotage, there are limited ways a threat actor could conduct logical espionage of the Piql Preservation Services. The first alternative is to install spyware in the Piql IT system. It would only be necessary to get past the security code in the Front-End service before they would have access to potentially valuable client information being prepared for writing. After having gained this unauthorised access, the spyware could view and extract the relevant pieces of information for later reading by unauthorised persons. The act of espionage does not necessitate the instalment of malware which alters or somehow damages the information, so its integrity would remain intact. The confidentiality of the information, however, is grossly compromised. It can be bad enough that the information is accessed and read by someone else, but worse still is that we can assume the threat actor now privy to the information is someone the data owner least of all wanted to have access.

The same loss of confidentiality would be the result when the second alternative is used. Spying on the contents of the Piql Preservation Services can also take the form of a threat actor using transmitters and receivers from outside the facility to gather information as it is transferred electronically.

9.1.16 Threats to Computer Security

We have previously in this chapter alluded to risks related to the operational IT system security architecture which will be implemented by Piql partners. These are especially present during the production phase, but some also during storage. The system architecture was laid out in chapter 5. Here, we point to possible weaknesses or holes in the setup which a threat actor with abilities to perform logical attacks may exploit to gain access to the system. Though we stressed that the security mechanisms demanded of the Piql partners by Piql AS are relatively strong, there are three weak points we would like to consider in the Piql IT system.

Firstly, there is the issue of the security code of the Front-End service. It is nearly impossible for FFI to analyse the reliability of the different security software employed here, especially when considering our 500 year perspective. Within the digital world, these things are extremely volatile, and software solutions are constantly tweaked and evolving as a result. The security software in Piql AS' system architecture may change in just a few years, and perhaps very soon the HTTPS protocol for secure connection which many of us are accustomed to now may be obsolete. The best the Piql partners can do is always strive to keep up with the latest developments in the technology, update their software regularly, run the Piql Preservation Services in a professional way so as to instil trust, and maintain the best way of operations as possible. Some of these instructions we will come back to later in the next chapter concerning recommendations. Always keeping the security software state of the art, as the current setup is, is a way to ensure that the Front-End service is as impenetrable as can be.

The second vulnerability was illustrated in the scenario describing sabotage, namely how a threat actor can gain access to the entire Piql computer system, not just the computer connected to the outside world with the external interface accessible to clients, to tamper with and alter the digital information stored in the system before printing. The reader will remember that the Piql IT system consists primarily of a Piql (reception and processing) computer and a Piql I/O (production) computer, which are physically interconnected through Ethernet cables. They also share a common hard disk which utilises an NFS.[41] The act of sabotage described here entails making the two computers logically connected, creating a connectivity which was purposely blocked in the initial setup of the IT system. This, however, is an act of sabotage which requires formidable hacking skills. As mentioned above, breaking through the Front-End security code is, while no small matter, something many can achieve. Creating a connectivity in the manner described here, however, is not an easy achievement.

With the current security architecture during the production process, a checksum is created on the CPU (Central Processing Unit) of the Piql (reception and processing) computer when client data is received and prepared for writing. This checksum is the same on the CPU of the Piql I/O (production) computer. During verification, which is done right before the writing process onto the piqlFilm is started, the production computer's CPU checks the digital file it has received through the NFS against the checksum created on the processing computer's CPU. If a threat actor has done any alterations to the information before it was stored on the NFS, this verification process will detect it, as the checksums will no longer be identical.

If, however, the threat actor has managed to create connectivity between the two computers, they have logical access to both computers' CPUs. It is then possible for the threat actor to alter the client data and the corresponding checksum on the processing computer's CPU, and also go in and alter the settings on the production computer's CPU to show the same altered checksum. The client data is thus no longer safe from attacks on its integrity. This is, on other words, a potentially disastrous vulnerability, but as it necessitates a threat actor with quite substantial abilities, the risk is not really that great.

The third weakness in the Piql IT security architecture has to do with cryptography, and it is a key issue. Today, Piql AS provides no cryptographic protection of the information of the piqlFilms.[42] A user of the Piql Preservation Service can, however, encrypt the data before transferring the files to the Piql partner if they wish. Yet, this is then done at their own cost and risk, and the user is responsible themselves for managing and storing the personal key.

In not offering cryptographic services themselves, Piql AS is offering a weak information security setup – especially regarding confidentiality – and implying that their clients are free to do so themselves does not make up for that fact. Indeed, placing any sort of responsibility for – and functionality of – IT security related to their service outside their own system is ill-advised. Who is to say what will happen if and when an encryption key is lost? Who will be responsible for the unsecure preservation of the information?

Of course, there is a reason why Piql AS does not wish to provide cryptographic services as part of the Piql Preservation Services: the concept of self-containment. Piql AS wants the information preserved using their service to be self-contained, in keeping with the principle of

[41] See figure 5.3 in chapter 5 as a reference.
[42] The information regarding cryptography was given during a meeting with Alfredo Trujillo, Product Manager at Piql AS, and Tore Magne Skar, Project Manager at Piql AS, on 23.11.15.

500 year longevity. What good is a longevity of this magnitude if the information cannot be accessed in the future without additional references?

However, this trade-off between security issues and the concept of self-containment should be up to the user to decide. If a user, for instance a national archive, wishes their information stored on the piqlFilms to be accessible to all, also in the future, then cryptography is a non-issue and the concept of self-containment is paramount. If, however, a user, perhaps a competitive business storing patents, wishes their information to remain secret or private no matter what, then cryptography is vital. The decision depends on whether the user values availability or confidentiality the most.

Piql AS' current security architecture addresses integrity – through the measure of verification – and availability – by not deleting the original file from their computer system until the production process is complete. Conversely, they do not offer anything to address confidentiality. Though this may run counter to their vision for the Piql Preservation Services, not at least offering it as a part of their security architecture for users to choose is a weakness.

Apart from the abovementioned weaknesses in the Piql IT system, there are also some worth mentioning in the piqlVault IT system during the storage phase.

As mentioned previously in this chapter, the only real logical threat to the piqlVault system is sabotage in the form of a threat actor gaining access to the system and wreaking havoc in the piqlVault grid. They can create complete chaos with regards to the locations of piqlBins within the grid and thus affect the availability of the piqlFilms, but the information security properties are not otherwise affected. It was also said that a threat actor had two ways to achieve this level of chaos. In the following we discuss how these events can come to pass by highlighting the exploited vulnerabilities of the piqlVault system.[43]

The first option was to gain access to the piqlVault IT system through the potentially vulnerable B interface network between the Piql IT system and the piqlVault IT system and install malware in the EWMS which switches the reel IDs around or orders random pick-ups continuously. The mere role of the B network as an interface between the two systems makes it a point of vulnerability. However, it seems that the setup it delivered from the supplier as a robust system when it comes to computer security, and it is up to Piql AS and their realisation of the system to keep it secure. It seems that Piql AS has done just that. Yet, such an interface can always be turned into the chink in the otherwise solid armour and exploited by threat actors with the proper know-how.

The second option was to affect the radio signals controlling the movements of the robots through the use of a malicious transmitter. The use of a 2.4 GHz frequency to send the radio signals through enhances security, as there is less radio propagation of the signals. However, FFI has not learned of any cryptographic methods used in the information in the signals. Without this feature the information in the signals can be accessed and possibly distorted. With

[43] See figure 5.4 in chapter 5 as a reference.

the use of a malicious transmitter, then, a threat actor could either jam the signals completely and halt all operations, or, if the threat actor is able to break through the security protocol protecting the radio signals, their contents can be altered to make the robots move about haphazardly all over the piqlVault grid. We mentioned in section 5.5.3 that the security protocol used by the radio signals is a protocol of the supplier of the AutoStore® system's own design, the contents of which FFI has not been privy to.[44] The fact that the protocol is not standard, i.e. that its contents are unknown, amounts to a certain degree of security, but it is a weak form of security. As FFI does not know its contents, we cannot assume it is impossible to breach.

Having outlined the relatively few weaknesses to the IT security architecture of the Piql Preservation Services, we now turn to a discussion of the importance of a sound security architecture along three different viewpoints: that of the client, of Piql AS, and the supplier of the piqlVault system. The consequences of the potential loss of information is different for the three, making the risks associated with the loss vary in severity.

The client or user of the Piql Preservation Services is perhaps the one which stands to lose the most should something happen to the CIA of their information stored. They are also affected should something happen to all three types of data stored with the Piql Preservation Services: the client data (content data), metadata and unique film reel IDs.[45] Piql AS must strive to earn the trust of the clients in the service that they provide, meaning that the client can trust that Piql AS' IT security architecture is up to par, and they can trust Piql AS to make sound judgements when it comes to the suppliers and providers they choose to outsource parts of their service to. If the clients cannot trust the functionality or security of the Piql IT security architecture on these issues, several things can happen which would have very negative consequences for them. First, if Piql AS' computer security fails, the clients can potentially lose their content data, or the metadata which allows this data to be located, or the reel ID which allows the physical film to be retrieved. This would affect the CIA of the data. Second, if something fails in the IT security architecture of the supplier of the piqlVault, it will be impossible to find a given reel exactly when needed. This would affect the availability of the data. The client is thus vulnerable to mistakes in both the internal Piql IT system and the external piqlVault IT system.

For Piql AS themselves, the risks are similar to that of the clients, as they also are affected if something happens to all three types of data. If there is a security breach in the piqlVault IT system which affects the reel IDs stored there, and they are then unable to extract the piqlFilm, this reflects negatively on Piql AS' business image. As a result, Piql AS may lose trust from their existing and potential new clients, which, as mentioned above, is vital to keep. Though Piql AS must maintain a good relationship with their clients in this capacity, they must also be sceptical of what the clients might bring into the Piql IT system, either wittingly or unwittingly. Should a threat actor posing as a client, or threat actors in general, be able to ingest malware in the Piql IT system through the Front-End service, this could negatively affect both the content data and the metadata.

[44] The information regarding the security protocol designed by Hatteland was given during a meeting with Terje Skjølberg, Sales Manager at Element Logic AS, on 11.11.15.
[45] See figure 5.3 in chapter 5 as a reference.

Finally, the supplier of the piqlVault system is the smallest stakeholder in the functionality of the Piql Preservation Services. The only type of data they have access to, and are thus affected by, is the reel ID and local ID used in the piqlVault system. A security breach here would only result in loss of availability of the information stored, not its integrity, and would only damage the business image of the piqlVault provider.

10 Alternatives for Digital Storage

10.1 Existing Digital Storage Technologies

This report consists of a risk assessment of the Piql Preservation Services, where its functionalities and security qualities have been described and analysed in a security context. To give the reader a better understanding of the properties of the Piql Preservation Services, this chapter will place the system in a wider context and relate it to the other technologies of digital storage which are used commercially today. We first give an overview of the existing storage media available today and an introduction to their qualities, particularly with regards to their storage capacity and longevity. Next, we briefly assess their security qualities compared to the Piql Preservation Services before, finally, certain features of the Piql Preservation Services are outlined, which illustrates how it is better suited for long-term preservation.

The storage media included in this brief presentation of alternatives for digital storage are hard disk drives (HDD), optical disks (CD (Compact disc)) and magnetic tapes (LTO (Linear Tape Open)).

10.1.1 Hard disk drive (HDD)

Hard disk drives (HDD) have been the main form of persistent data storage in computer systems for decades, and much of the development of file system technology is predicated on their behaviour. The HDD offers a cost efficient and easy accessed way to store and retrieve data. The data is recorded by magnetising a thin film of ferromagnetic material [57]. Hard disks consist of one or more metal platters mounted on a central spindle where each platter is covered with a metal coating. The entire unit is contained in a sealed chamber. The number of platters included, and the density of the bits in the device, decides the storage capacity of a hard disk. The maximum storage capacity is 10 terabyte (TB) per disk [57, 58].

There is one obvious disadvantage to the HDD: To gain optimal performance of the hard drive the read/write heads must be extremely close to the disk without actually touching it. This means that a human hair, a dust particle or even a fingerprint can bridge the gap and cause the head to crash, which can destroy the data in the area of the crash [59]. These high failure rates make hard disks inappropriate for long-term preservation. Due to the relatively short lifespan of the HDD – the average lifespan is six years – and the high failure rates, it is common to make use of several disks, known as RAID (redundant array of independent disks), in order to ensure data redundancy and minimise the risk of data loss [60, 57].

10.1.2 Optical disk (CD)

Optical disks (CD) are flat circular disks that encode digital data on one of its flat surfaces [57]. An optical disk drive uses a laser light to write data onto or read data from an optical disc, which includes CDs, DVDs and Blu-ray disks [61]. One version of the medium – CD-R or DVD-R – writes the information onto the CD or DVD only once but enables the information to be re-read many times, whereas another type – CD-RW or DVD-RW – allows new information to be rewritten onto the same medium. If the former is used, the data is immune to corruption for the longevity of the medium. Optical disks are cheap and easy to use and are most commonly used for distribution and storing of published software and games, as well as audio and video recordings [62].

Compared to other storage devices, optical disks offer low data capacity with a maximum of 700 megabytes (MB) for CDs, 8,4 gigabytes (GB) for DVDs and 50 GB for Blu-ray [63]. Their lifespan varies depending on whether they are recorded or not: the lifespan of an unrecorded CD is 5-10 years, whereas the lifespan of one with content is 2-5 years [64]. These features illustrate how optical disks were not originally developed for long-term preservation, but rather as a mass consumer product. Making use of optical disks in a digital archive requires a significant investment in knowledge and technology, which is why they are better suited as a digital storage technology used for a limited period of time. They are not a permanent solution, as both future developments in technology and the deterioration of the optical disk over time will necessitate the migration of the disk's content onto a new medium. CDs and DVDs are fragile and may snap or scratch easily, in addition to being affected by environmental factors such as dust, heat and UV light [57, 62].

10.1.3 Magnetic tape (LTO)

Magnetic tape is an analogue medium for magnetic recording, made of a thin magnetisable coating on a long, narrow strip of plastic film. The magnetic coating makes it possible to retain electronically encrypted data in digital format [57]. They use serial access to find a piece of data, which makes it fairly time-consuming to find and retrieve data. Therefore, it is most appropriate to use magnetic tapes for storage of data that is not likely to be needed instantly. Another disadvantage is that the data on the magnetic tape may be corrupted if the tape is placed near a strong magnetic field, e.g. a large speaker or a magnet.

Magnetic tapes can store up to six TB of uncompressed data [65]. Their lifespan is up to 30 years under optimal storage and handling conditions, but this really only applies when the store-and-ignore principle is put to use, i.e. that the digital data is transferred to the medium and then hardly accessed again. When one includes the added wear and tear of a magnetic tape that is in use, a more realistic lifespan is about 10-20 years. Still, due to the delicacy of the material, where even small particles can cause damage to the medium, few wait that long to migrate the data onto a new tape. The market “best-practice” is to migrate the data every 5-10 years [57].

10.2 Security Qualities

Although we have not done a similarly thorough review of the security qualities of these alternative digital storage media as that presented in the previous chapter of the Piql Preservation Services, it can be safe to assume that they would not be able to withstand the negative effects of the worst case scenarios we have just outlined. We can assume that the different media would all be vulnerable to the effects of excessive heat cause by fire; by filthy water; by the crushing physical pressure of overhead weight; and by chemical compounds and harmful microorganisms. Similarly, we assume none are immune to neither the threat of the insider nor to physical theft or sabotage.

With regards to the issue of radiation, though, the different storage media are affected in different ways. As our analysis has shown, the piqlFilm and piqlBox are immune to exposure to electromagnetic pulses. Because no magnetic fields are involved in the writing or reading processes during production, it is unaffected by electromagnetic radiation. The same is the case for the optical disk [66]. The situation is quite another for both the HDD and the LTO. Both are highly affected by any devices which create a strong magnetic field. The reverse, however, is true where it comes to the effects of UV radiation. In this case, the HDD and LTO are unaffected, whereas damage can be done to the data stored with the Piql Preservation Services or a CD or DVD when exposed to too much UV radiation from the sun or overhead lights [62].

10.3 Long-Term Preservation

There is one area where the qualities of the Piql Preservation Services set it apart from the other storage media, and that is regarding its true long-term preserving abilities [67]. Of the three alternative storage media presented above, only the magnetic tape seems well suited for similar long-term storage usage. Yet, due to its relatively short lifetime expectancy, its application seems better suited for archival purposes rather than for preservation purposes. When it comes to preservation – understood as maintaining something in its original or existing state, keeping it alive and keeping it safe from harm or injury [44] – the Piql Preservation Services is the most appropriate storage method for long-term preservation of digital data available today, provided that the piqlFilm is stored under the proper storage conditions.

The Piql Preservation Services is the technology which is best suited for long-term preservation because it is migration-free, unlike the other storage media. Because of the deterioration of the alternative storage media over time due to environmental factors and general aging of the material, in addition to continuous developments in software, hardware and file formats, migration of the data from one medium to a new “healthy” medium is needed at frequent intervals. This is not the case for the piqlFilm. It has a proven longevity of at least 500 years, which eliminates the need for data migration [3].

As a migration-free solution, there are many benefits to the Piql Preservation Services. Firstly, there is the matter cost efficiency. The need for data migration is very costly. As the volume of digital data which needs storing is growing, so is the storage infrastructure surrounding it. This means that the complexity of data migration is increasing, requiring fresh materials for the storage media and becoming more labour intensive [68]. A lot of resources can be saved, in other words, if this need is removed.

However, the benefits relating to increased security, which come as a result of the Piql Preservation Services being a migration-free solution, is of the most importance in this report. Due to the longevity of the piqlFilm, the risk of migration-related data loss is avoided. The data is not lost as a consequence of the decay of the medium storing the information, and neither will it be corrupted or manipulated during the migration process. The piqlFilm is a true WORM technology, meaning that the film is unalterable; once the data is written it cannot be edited [3]. As there is no need to rewrite the data onto a “healthy” piqlFilm every few years, this makes it impossible to manipulate or delete data on the piqlFilm once it is written.

This is connected to another major security feature of the piqlFilm: As no migration of the data is needed once it is stored on a piqlFilm, the data is not connected to external networks for longer than strictly necessary, i.e. during production. This greatly reduces the opportunity of a threat actor to logically manipulate or steal the data, which is a major risk when it comes to information security. With alternative storage media, the digital data must be connected to external networks at regular intervals or the data owners stand to lose the data once the storage medium is no longer readable.

11 Recommendations

In the scenario descriptions, which are attached to the report as appendixes, we have briefly listed suitable recommendations to alleviate the risk source identified in the scenarios. In this chapter we provide an overview of these recommendations. We begin by giving some general recommendations and continue with more specific recommendations on how to alleviate the risks to the physical properties of the Piql components, and, lastly, some recommendations concerning computer security.

We make recommendations on security measures in general which the Piql partners can implement to keep the piqlFilms they store as protected as possible. We also make additional recommendations to the Consortium partners of alterations to the Piql components, which they may decide to use in later work packages of the PreservIA project.

However, the recommendations are not binding: they are meant only to serve as guidelines. Because the risks faced by different user of the Piql Preservation Services vary depending on geographical setting and sector, and they also judge the severity and acceptance of the risks differently among themselves, there is no “one size fits all” model. We have identified the risks faced by the Piql Preservation Services in general, and it is up to the individual users to decide how they need to prioritise them. The only exception is when we give recommendations which specifically suit the needs of the high demanding user. Generally, it is only necessary to put in place enough security measures in and around the Piql Preservation Services to deter threat actors with the intention to compromise the CIA of the information from acting. How many measures that amounts to, is adjustable to the different market areas and the level of sensitivity on the information, and is up to the users and Piql partners to determine specified to their circumstances.

11.1 Recommendations for General Security

A general rule of information security is to always keep backups [16 p.46]. If one wants to be truly secure, one should request more than one copy of the piqlFilm. The backup copies must be protected in the same way as the original copy, and preferably placed in a different location. This will amount to an additional cost, but security does cost. This issue will always depend on how valuable the information is to a person or entity.

Another general measure to employ when using the Piql Preservation Services is to preserve the information using the hybrid method, i.e. both as visual text and pictures as well as digitally encoded data. By printing all the information twice on the same piqlFilm it is easier to determine that the information is the same and has not been tampered with, for instance if a few frames of the piqlFilm have been cut away after it was written into its physical form. The integrity of the information is thus doubly ensured.

We stated in chapter 9 that the piqlFilms are at their most vulnerable when they are “out in the open”, and this makes the transportation phase particularly hazardous. Other than to change the routes of the transportation from day to day so as to take away a threat actor’s ability to plan precisely where to stage an assault, there is additional measure that can be taken and that is to eliminate the transportation phase altogether. To achieve this, the production site must in effects be moved to the storage facility, including all necessary printing equipment and know-how. For a user storing very sensitive information, it may be worth the additional effort.

Tied to the risks present during transportation is the recommendation to always be aware of your surroundings, though this recommendation is valid for the placement of the piqlVault or production site as well. The Piql partners should avoid placing their services near high risk occupancies, such as near industrial plants or dams. If such placement is unavoidable, the Piql partners should always take the necessary precautions connected to the risks presented. Even if the circumstances of the Piql Preservation Services are deemed to be relatively safe and secure, the Piql partners should always have the required safety and security measures in place, because we can never know what the future might bring, neither with regards to climate change, or if a chemical plant is built in the vicinity or if someday someone decides to bomb a neighbouring business. If the piqlVaults and production sites are protected from the risks we can predict, they should be well-prepared for most of the ones we cannot.

The inside threat was highlighted in chapter 9 as one of the biggest security challenges the Piql Preservation Services faces. Fortunately, there are several things that can be done to mitigate this threat:

1) One can make sure sound procedures for vetting of potential employees are in place during the hiring processes. These can include full security clearance or criminal record and credit check depending on sector.
2) It is important to perform such checks at regular intervals, not just at the start of the employment. This is to ascertain whether any changes in circumstance has come about which can have a negative effect on the way an employee conducts him- or herself at work.
3) It is possible to put in place even stricter procedures when it comes to accessing certain parts of the service, making sure only a few highly trusted people have access to the most critical parts of the service.
4) Some sort of control system can be implemented which ensure that the piqlFilms cannot be removed from the grid without being signed out by a second Piql operator.
5) Similarly, a control system can be implemented which does not allow piqlFilms to leave the storage facility unless authorised by two or more authorised personnel.
6) A working schedule can be worked out which ensures that no one person works alone. This applies to the writing process, during storage and it applies to the security personnel. For instance, a Piql operator working alone can simply put a memory stick into the computer and download the original file, and a security guard working the night shift can be bribed to give unauthorised access to threat actors.

Besides these specific measures, mitigating the inside threat mostly comes down to building a relationship of trust between employees.

In chapter 5.4 of this report, when we outlined the location and description of the piqlVault, we alluded to the fact that perhaps not all users would wish to store their sensitive information in a regular office building. We were referring to the so-called high demanding user. When such users believe that a regular office building will not provide sufficient safety and security measures, our recommendation is to instead place their piqlVault system in a mountain repository.[46] The additional safety and security benefits of placing the information in a mountain hall include the location, which is somewhere off the beaten track, the exact location possibly being unknown to most people, multiple backup generators as energy redundancy, and fortified walls with additional protection against a nuclear blast, radiation, electromagnetic pulses and CBR agents. If the user does not have access to storage facilities such as these themselves, it is possible to rent a room in a mountain hall, which is called hosting.

[46] The high demanding user may also wish to use a manual storage system instead of an automated one.

11.2 Recommendations for Physical Security

Chapter 9 emphasises loss of ideal storage conditions as another key risk presented to the Piql Preservation Services. First, we give a recommendation which concerns maintaining the storage conditions on a day to day basis, and not one which concerns what to do in a crisis: the piqlFilms should not be stored in a room which is adjacent to other rooms housing a lot of electrical equipment. In these situations there is a risk of heat dissipation from the machines which could affect the temperature of the storage room. The risk of a potential electrical fire reaching the storage room is also greater.

The events which can cause loss of ideal storage conditions are loss of utilities, which causes the ventilation system to stop functioning, or because of damages to the building's infrastructure, which exposes the piqlVault to the elements outside. If the latter, the measures a Piql partner can take are elaborated upon below in the paragraph concerning physical pressure on the piqlBox and piqlFilm. If the former, the main measure to mitigate the situation is to have redundancy of the supply of utilities into the piqlVault. Of most importance here is redundancy in energy supply, but the same logic applies to water, gas, etc. Both backup generators and doubling of energy supply from two independent sources in the area are recommended. If a larger area is subject to a complete blackout, a redundant energy supplier may do little good, whereas a backup generator powered by for instance diesel will be functioning.

In case of fire, Piql AS' recommendation to use an oxygen reduction suppression solution as the fire protection mechanism in the piqlVault is regarded as the best one. Making sure the supply of the oxygen restricting gas is such that it can withstand prolonged fires is also important. Though all Piql partners are required to have some form of fire protection in place, not all are suited for implementation in the piqlVault. A sprinkler system, for instance, could potentially do more harm to the Piql Preservation Services than the fire it is meant to put out. With regards to mitigating the effects of a forest fire, this is mostly about taking precautions where it comes to the construction of the building housing the piqlVault or production site and its surroundings, such as clearing a safety zone between structures and combustible vegetation and using only fire-resistant or non-combustible materials on the roofs and exterior surfaces, among other things.

As described in the scenarios illustrating the effects of fire, the plastic of the piqlBox and piqlFilm will burn if they come in too close proximity to the flames. A protective measure which the Consortium partners in the PreservIA project might consider is adding some sort of flame deterrent to the piqlBox. If the piqlBox is fire-resistant, there is less risk of the fire damaging the piqlFilm inside.

The effects of water on the piqlBox and PiqlFilm are, as we stressed in chapter 9, an issue on which we do not have sufficient information to make clear statements. An absolute key recommendation to the Consortium partners is therefore to conduct testing specifically on the piqlFilm to learn more about its reaction to water, which in turn can allow us to alleviate potential negative reactions. It is important to test the effects of clean and dirty water, of hot and cold water and different duration of submersion.

Despite lacking this information, our recommendation is still to avoid any exposure of the piqlFilms to water. To extinguish fires, rather use the oxygen reduction suppression solution recommended by Piql AS, or another fire protection mechanism which does not involve the use of water as an alternative. When it comes to flood mitigation strategies, these include elevating the structures which house the piqlVault in flood-prone areas, or, if that is not possible, placing the piqlVault on upper floors of the building.

Should the piqlFilms nevertheless come in contact with water, Piql AS recommends that they be kept wet, and brought to a proper facility for re-washing and drying before they are handled again. This is to prevent the film layers from sticking together, as well as the growth of bacteria. Additionally, it can prevent swelling and softening of the emulsion, which can cause major damages [27].

The most apparent recommendation we can make to prevent the negative effects of water on the piqlFilm is to make the piqlBox air-tight, i.e. water-proof. Barring that, a protective measure which the Piql AS can offer the higher demanding user is to seal the piqlBox in external bagging or wrapping. The PreservIA Consortium has developed a solution where the piqlBox is wrapped, vacuumed and sealed in an aluminium foil, which should solve the issue of both splashes or sprays of water and if the piqlFilm is submerged in water.

As is the case with the effects of water, there is insufficient information regarding the effects of external physical pressure on the piqlBox and piqlFilm, and how particularly the piqlFilm is affected by jolts and drops. Similarly, our clearest recommendation is to conduct tests to the effects of these issues, in order to get a better understanding of the consequences thereof. In the scenarios concerning these issues, we have emphasised falling infrastructure as a possible cause, due to, among other things, earthquakes. To this matter, at least, it is possible to give some general recommendations which can increase seismic resistance. Many of the recommendations concerns making the structure of the building stronger in general, which could also mitigate the effects of, say, an explosion. Seismic resistance can be accomplished through for instance fortified walls with braced frames and energy dissipating devices such as viscoelastic or elastomeric dampers [69].

In chapter 9 we described how neither the piqlBox nor the piqlFilm is likely to withstand exposure to chemical compounds. Particularly the negative effects of strong oxidative chemicals like ozone is something the PreservIA Consortium is currently testing and working to mitigate. Although the piqlBox is biologically inert, the same result can be expected for the piqlFilm from exposure to harmful microorganisms as with chemical compounds: the gelatine emulsion layer reacts violently and the integrity of the information stored is completely destroyed. A possible solution to help protect the piqlBox and piqlFilm from these risks is the same as with water: wrap the piqlBox in a sealed aluminium foil to ward off gases, bacteria or other microorganisms. Its protective properties against these risks have not been verified, so it needs to be tested. If its functionality is proven, however, the Piql partner can, as we say, kill two birds with one stone.

We now move on to recommendations to alleviate the effects of radiation, both nuclear and electromagnetic, as well as ultraviolet. The effects of nuclear radiation on the piqlBox and piqlFilm were, as we saw in chapter 9, not very severe. Additionally, the likelihood of this issue becoming a reality for the Piql Preservation Services, both as a consequence of an accident at a nuclear plant or a nuclear detonation, is too low to make radical changes to the safety and security measures surrounding the Piql Preservation Services. Hence, we make no specific recommendations on the subject. The same applies to the issue of electromagnetic radiation. If weaponised and directed specifically at the Piql Preservation Services, the electronics in the system will be negatively affected for a time. However, we have seen that the piqlBox and -Film are not affected, i.e. no harm is done to the confidentiality or integrity of the information stored, just possibly its integrity. No specific recommendations are therefore made, except to advise the Piql partners to prepare for the possibility of failing electronics, as we are sure is done regardless of the risk of electromagnetic pulses. The dangers of ultraviolet radiation, on the other hand, are something that must be taken into account. This can affect the integrity of the information on the piqlFilm quite severely, and our recommendation is therefore never to leave the piqlFilm exposed to sunlight and to use appropriate lighting inside, as specified by Piql AS.

When it comes to physical theft and physical sabotage, the best ways to mitigate these threats is to ensure a sophisticated security regime is in place in and around the piqlVault and the production site. As both types of risk presuppose the physical presence of a threat actor, the best mitigation is to make sure they are unable to enter the facilities, and if they do, put enough obstacles in their way to thwart their mission that way. The security regime as stipulated by Piql AS and a strategy for its implementation by FFI is described in section 5.5.2 of this report. Apart from following our recommendations with regards to mitigate the risk of the insider – in this case an insider either performing the acts of sabotage or theft themselves, or enabling others to do so – we advise the Piql partners to consider the following reinforcements of the security regime as well.

To start with, it is possible to implement better perimeter control than what is stipulated by Piql AS, in the form of fences or walls around the facility, gate monitored by security personnel for admittance and turnstiles or other forms of sluices which are controlled through ID verification solutions and camera surveillance. Besides this addition, the camera surveillance scheme proposed by Piql AS is sound, as is that addressing alarm systems. With regards to security personnel FFI would add a recommendation of employing a guard during office hours as well, and adding an additional guard outside of office hours as well, both for enhanced protection but also to mitigate against the inside threat.

11.3 Recommendations for Computer Security

The recommendations we make with regards to computer security is to mitigate the threat of both logical theft and sabotage, as well as logical espionage.

As a general rule and a way to ensure the most impenetrable computer security regime possible, our recommendation is to the guidelines set forth by the Norwegian National Security Authority [70]. Our view is that the routines of best practice laid out here must be in place. There are four main guidelines and six additional ones. These stipulate: make sure that all hardware and software is state of the art; update new security software as fast as possible; never distribute administrator rights to end-users; and block any and all running of unauthorised programmes. According to NSM, studies show that these four measures stop about 80-90 % of all internet related attacks [70]. The additional six guidelines stipulate: activate code protection against unknown vulnerabilities; harden applications; utilise firewalls on client interfaces; use secure booting and hard disk cryptography; use antivirus and anti-malware; and never utilise more applications and functions than strictly necessary.

Chapter 9 pointed to a minor flaw in the Piql IT system regarding the physical connectivity between the Piql (reception) computer and the Piql I/O (production) computer. One of the scenarios in the scenario analysis describes how a threat actor can utilise this connectivity to create a logical connection between the two computers and as a result alter the information being written onto the piqlFilm. To mitigate the effects of this, constant monitoring is required. Another option is to create a true air gap between the two computers' CPUs, i.e. use a USB memory stick or the likes to transfer the files between the computers. Although this will not stop the threat actor from gaining access into the Piql IT system, it will make it impossible to alter the received client data undetected. However, such a measure is an unlikely feature of a production process, as it would make the production too inefficient, but it is food for thought.

Verification of the integrity of the digital file upon receiving it from the client and after it has been prepared for printing is key. Piql AS already has this measure included in their security setup, and the recommendation is to always ensure that it is state of the art.

The last recommendation we make to Piql AS and to the Piql partners is regarding cryptography, a recommendation we also elaborated upon in chapter 9. Our view is that any computer security architecture which does not offer cryptographic methods is an unnecessarily weak one. Though it would compromise Piql AS' vision of the Piql Preservation Services as self-contained, whether this feature should be intact or not should be up to the individual user to decide. Measures should be implemented to protect the information also after it enters the Piql IT system, not only at the Front-End Service before it enters. Piql AS should therefore offer this solution to its users, though not all will want to utilise it. A caveat is, however, appropriate to issue here. Though FFI recommends cryptography to be part of the service which Piql AS offers their user to enhance security, we have no way of knowing how secure cryptographic methods will be considered in the future, i.e. how easy it would be to break the cryptographic code. Nevertheless, for the present this is the keenest recommendation we can make to ensure the confidentiality of the information stored using the Piql Preservation Services.

12 Conclusions

FFIs assignment in the PreservIA project has been to identify vulnerabilities and security challenges faced by the Piql Preservation Services today and in the next 500 years. As it is difficult to analyse something we cannot observe, we have had to base our assessment on risks and threats present in the foreseeable future. We have, however, tried to include a longer timeline by including scenarios which account for a high degree of uncertainty, such as terrorism, armed conflict and nuclear war.

The vulnerabilities and security challenges which were identified in the scenario analysis may seem numerous, and, as such, paint a bleak picture. However, the outlook is not so grave. We have deliberately chosen to include descriptions of worst case scenarios in the assessment, and many of the vulnerabilities identified will only materialise under the worst of circumstances. Often there is also an easy solution to the problem. Our aim for presenting the vulnerabilities in this fashion is simply to emphasise that the event which so negatively affected the Piql Preservation Services *can* be a risk, so that Piql AS and Piql partners supplying the service are aware of the dangers and are consequently motivated to plan for them.

Our scenario analysis identified several vulnerabilities: some severe, such as fire, chemical compounds and the threat of the insider in theft and sabotage; some not so severe, such as the effect of electromagnetic pulses and nuclear radiation; and some which simply require more testing before we can say anything definitive about their effects and consequences for the information stored with the Piql Preservation Services, such as the effects of water, smoke and physical pressure. Additionally, the PreservIA Consortium will conduct more tests regarding the effects of oxidative chemicals, such as ozone, which will enhance our understanding of how the piqlFilm reacts when exposed to chemical compounds.

The main finding of the assessment with regards to identifying vulnerabilities is that the gelatine emulsion layer on the piqlFilm is the weakest link. As this is where the information is written, this vulnerability can have grave consequences for the security of the information stored. Though it does not stand to affect the confidentiality of the information, it highly influences the integrity and thus availability of the information. It should be noted, however, that the gelatine silver print method – preserving information using silver halides in gelatine on a base – is a technique that has been in use since 1874 to preserve photographs and later moving images [71]. Despite imperfect environmental conditions, such images still exist today, implying that this technology has withstood the test of time and proven its basic robustness.

Nevertheless, the Piql Preservation Services has many strengths. For instance, though it seems like the gelatine emulsion layer is very vulnerable to external influences, the choice of material for the rest of the Piql components – the plastic of the piqlFilm, piqlBox and piqlBin – can serve to increase the security of the information stored. Especially the properties of the PP of the piqlBox and the PET of the piqlFilm seem to be able to withstand a great deal of external influence, and their longevity is proven [3].

Another choice made by Piql AS that has enhanced the security and safety of the Piql Preservation Services – a subject we have touched upon in some sections of the report already – is the choice of an automated storage system: the modified piqlVault storage system. This does seem like a very robust choice of storage system which may eliminate many risks. Firstly, the design of the piqlVault system grid seems quite stable and cannot easily be tilted or overturned. This stability is strengthened by the tight stacking of the piqlBins within the grid. In this way, the piqlFilms are better protected from falling to the floor and being damaged as a result than if they were stacked on shelves. Secondly, it seems more difficult for an outsider to simply grab a piqlFilm reel and run. Should a threat actor be able to break through the security regime and is able to gain access to the storage room, the piqlVault system will serve as an extra obstacle, as one also needs to be able to work the system in order to extract anything from it. And thirdly, the system seems better protected against human error. The risks of human error causing damages to the piqlFilms decreases with an automated system, as the piqlFilms are exposed to potentially dangerous situations less often when handled by machines than if personnel were the main way of handling the piqlFilms.

An additional, and perhaps the most significant, strength of the Piql Preservation Services is being offline. As most other digital storage media, where the digital data is written onto a physical medium stored separated from online networks, there is limited opportunity for a threat actor to attempt to steal or otherwise harm the information stored on the piqlFilm by logical means. What sets the Piql Preservation Services apart, however, is the prolonged period of time in which is it offline, i.e. the fact that there is no need for the migration of the digital data onto a new “healthy” medium every few years. Such frequent migration requires more regular connection to online networks, as well as more parties involved with the management of the data. With the elimination of this need for migration, the content data stored on the piqlFilms has to be connected to online networks only *once*, and only a handful of people must ever be involved in the process of managing the data. The number of potential risk sources eliminated by the offline properties of the Piql Preservation Services is therefore great.

Another strength of the Piql Preservation Services which is tied to this topic is the relative solidity of the Piql IT system security architecture. Even when the content data is connected to online networks, the computer security mechanisms put in place by Piql AS are relatively strong – relatively in the sense that complete protection from all logical attacks of some kind is very difficult to achieve. In consequence, the client data is kept relatively protected throughout its journey with the Piql Preservation Services, at least with regards to computer security.

When it comes to physical security, there are some issues, but these are often a result of, and an inherent part of, being part of a larger context where external forces outside of your control – be it forces of nature or threat actors with malicious intent – can somehow affect you. Taking necessary precautions and constantly being alert and aware of potential risks should be sufficient. The risks to the Piql Preservation Services may be made to be even lower with time if alterations are made to the Piql components in later work packages of the PreservIA project as a result of this assessment. Risks may also be reduced if users apply our general recommendations of increased safety and security – adjusted to their needs and circumstances, of course.

Ultimately, the decision to store information using the Piql Preservation Services or in any other manner, is a matter of risk acceptance. There will always be risks involved with every storage system when valuable information is involved, it is simply a matter of placing the risk at a level which is acceptable to the user and implement measures accordingly. This would, of course, also be very different between users.

Appendix A Scenario Method

A.1 Definitions – Intentional Acts

The **actor** parameter describes the actors who could have the intentions and capacities to pose a threat to the Piql Preservation Services. The relevant values assigned here are state, network, company and individual.

A *state* is a sovereign political entity, meaning that it is subject to no one's laws but the ones they themselves choose to be subjected to. As such, it is the highest level of political organisation in the international system of actors.

A *network* is here understood as a form of organisation which lacks a formal structure with hierarchical levels and a clearly defined leadership. Rather, networks are made up of nodes. Some of the nodes may have a more central role than others, but they operate largely independently from one another. The nodes may be located in different countries, and cross-border operations are common where information and resources may flow across national borders, due to the advances made in telecommunications. A network may have an ideological or economic impetus. Examples of the former could include such wide varieties as terrorist cells and volunteering organisations, while the latter could include Mafias and cartels. A group, an organisation, a society or an association are here understood as synonyms to a network.

A *company* is any entity that engages in some form of business to make money, i.e. making, buying or selling goods or providing services in exchange for money [72]. Companies can be structured in different ways, but they all have a hierarchical structure with a clearly defined leadership which delegates tasks and manages its personnel in hierarchical levels from top to bottom. The level of responsibility and therefore liability is similarly diluted as we move down a level. A firm, a business, a corporation or an enterprise are here understood as synonyms to a company.

An *individual* is primarily understood as a person acting alone and on behalf of him- or herself, but nevertheless with the potential to greatly influence outcomes. He or she may also act with one or more accomplishes, and for reasons bigger than his or her idiosyncratic interest, but he or she is not connected directly to a larger context, such a network.

The **goal** parameter specifies the possible goals that a threat actor would hope to achieve, or the incentives for their actions towards the Piql Preservation Services. The relevant values assigned here are political power, market power, economic gain and idiosyncratic interest.

Political power can be gained from the possession of an object – in this case, the information on the piqlFilm – in the sense that the knowledge of what is on the film can give a threat actor increased influential power on a general level. An example would be if a state acquired instructions to build a new type of weapon system. Even without the intention of using said weapon system on a specific party, the general having of the weapon system can increase the state's influence generally on the world stage. It can also lead to increased authority in a bilateral relationship more specifically. The knowledge gained from the acquiring of the piqlFilm can be used directly to force certain behaviour, or indirectly when the counterparts' knowledge of you having the information is enough to give them an elevated position, even when they do not intend to make practical use of the information you have.

Market power is understood here as a more abstract notion than the financial reward to be had from economic gain. Market power is gained when an entity's standing in the market is increased, or its reputation in improved, without this being directly connected to an increase in profit. An example may be if an entity gets access to innovative technology.

When a threat actor acts due to motivation of *economic gain*, he or she does so because they imagine there is a financial reward to be had in acquiring an object – in this case, the information on the piqlFilm. The economic gain can be direct, meaning that usage of the object may result in direct potentially long-term profit, or it can be indirect, meaning that the object can be sold to a third party for a short-term profit.

If a threat actor seeks to gain possession of an object solely to appease his or her own wishes, they act out of *idiosyncratic interest*.[47] Such interests can be the destruction of the film for destruction's sake, perhaps governed by a wish for revenge.

The **method** parameter describes the actions a threat actor would take to achieve their goals. The methods vary regarding how demanding they are to implement, and thus represent different levels of ambition and capacity [39 p.13]. The relevant values assigned here are physical destruction, physical manipulation, logical destruction, logical manipulation and insider.

With regards to method, it is distinguished between physical and logical attacks on the assets in question, as well as employing the method of engaging an insider to do the job. As the Piql Preservation Services is both an online and offline medium during different phases in the service journey, it is subject to threats and hazards of both a logical [56 p.18] and physical nature: by logical threats or hazards we mean threats faced by the Piql Preservation Services while the information is stored or transferred electronically; by physical threats and hazards we mean all that may harm the physical infrastructure of the Piql Preservation Services, including its components and their critical dependencies. Within the separation between physical and logical we also distinguish between destruction and manipulation, as both types of attacks can result in the irreparable damage of the information or the subtle altering of the information.

Physical destruction entails damaging the medium containing the information, i.e. after the information has been transferred to the film, beyond repair. It also entails the destruction of other objects and materials that make up the Piql Preservation Services, such as the machines required to develop the piqlFilm, or the finer electronics of the piqlVault system. Additionally,

[47] According to The Concise Oxford English Dictionary [44], idiosyncrasy is defined as a mode of behaviour or way of thought specific to an individual.

it involves the destruction of all physical barriers which prevents or delays unwanted behaviour towards the asset that is protected, such as the fortified walls of the piqlVault, and all electronic equipment or solutions which support, combine with or replace the physical measures, such as access control card readers. An example of such destruction would be a very powerful bomb which obliterates an entire building.

Physical manipulation targets all the same objects and materials as physical destruction, but is less severe. The objects in question are not damaged beyond repair, but simply put out of action for a time. Manipulation is defined as being too subtle and requiring too much finesse to use indiscriminate weapons. Tampering with the physical piqlFilm to erase or add frames after it has been printed; tampering with the piqlWriter to adjust settings so that the printing process is altered; cutting cables to deactivate alarm systems or ventilation systems; performing unauthorised operations directly on a Piql Preservation Services computer that cannot be accessed remotely; setting off a small explosive device whose blast radius is easily controlled to break through a door; or simply pick the lock: all these actions fall under the parameter of physical manipulation. The storage facility and the production site, including their components and structural dependencies are somehow physically manipulated. The purpose of these actions is in some way to compromise the CIA of the relevant piqlFilms. The physical nature of the act must be stressed, however, meaning that the threat has to be physically present to perform the deed, either touching the entity or device in question or being in the necessary proximity to send or receive the necessary signals. We also define this parameter to include the physical removal of a piqlFilm without authorisation. In this way, the predetermined daily routine of the piqlFilm is altered, or manipulated.

Logical destruction entails irreparably damaging the information during the periods when it is not on the piqlFilm, i.e. either during ingestion or for a brief window during the data retrieval. Unlike the parameter requiring physical proximity in order to alter a process or object, this parameter consists only of operations that can be done remotely by gaining access to a Piql Preservation Services computer through hacks. Using various software tools, such as certain types of malware and viruses, entire files of information or just parts of the files are damaged beyond repair or deleted altogether.

Logical manipulation involves the same tactics as logical destruction, but here the purpose is not to destroy, but to gain access to embed malicious code, through the use of certain types of malware, in order to alter the information. Using the same reasoning as with physical manipulation, we also place the unauthorized logical extraction of data under this parameter, perhaps through the use of spyware. The sophistication of the Piql IT security architecture is such that we do not deem it possible for an individual without knowledge of the Piql Preservation Services, i.e. an employee, to gain access to the system.

Finally, the method *insider* entails engaging someone with intimate and unique knowledge of the Piql Preservation Services to perform the necessary operations, either physical or logical, in order for a third party to achieve their goals. By definition, an insider is someone privy to information unavailable to others, and, as such, can perform the operations with more ease and at a lesser risk and cost [44].

The **means** parameter describes the relevant resources a threat actor might employ to implement a given method, their capacities. The specific acts required of the given method are also briefly touched upon.

By *conventional weapons* we mean weapons that are in relatively wide use. There is a natural delimitation against weapons of mass destruction, which is elaborated upon below. Conventional weapons include small arms and light weapons, as well as common explosives.[48] Electromagnetic weapons (EMW) also fall under this category [55]. More primitive weapons, such as knifes, axes and the like, are also included in this parameter.

By *non-conventional weapons* we mean weapons of mass destruction, or weapons that are more indiscriminate in nature than conventional weapons. They include chemical, biological, radiological and nuclear agents (CBRN).

By *hand or power tools* we mean the tools or items one uses to physically do damage. Such tools include the items you would need to damage the physical or electronic infrastructure of the storage facility, for example if you wish to force entry. These tools do not refer to actions requiring the weapons described above. Instead, we refer to a pin or otherwise specialised tool to pick a lock, or pliers to cut a cable. Another example would be if one simply wishes to wreak havoc, for example by using a sledge hammer on a control panel which for instance puts various monitoring systems out of action. The tools and the level of competence required to use them have various levels of sophistication. Hand and power tools also mean such tools you would need if the purpose is to simply damage computer resources or hardware, without any hope of extracting any information.

By *malicious transmitters* we mean the equipment or device needed when the purpose is to damage or extract the information, but where such operations require physical proximity to be able to perform the act. Examples include, but are not limited to, malicious transmitters either clipped directly onto cables to receive the information flowing through them or transmitters handheld near enough to computer resources to receive the signals. The act and tools required to rewire certain cables are also included in this parameter.

By *software tools* we mean any kind of malware or spyware that can be placed on computer resources, as they are connected to wider computer networks and, as such, more susceptible to hacks. Here we refer to a hack as secretly gaining unauthorised access to someone else's computer for malicious purposes [72]. The malware and spyware can include, but are not limited to, viruses, worms, Trojans, fake antivirus malware, etc.

[48] For a more detailed listing of all the weapons that are included in the categories small arms and light weapons, see [73].

Lastly, by *monetary means* we mean means that are related to money or currency. Capital, in another word. This is a mean used when someone is payed to perform an action, often a malicious action, for you.

A.2 Consistency Matrix – Intentional Acts

	State	Network	Company	Individual	Economic gain	Political power	Market power	Idiosyncratic interest	Physical destruction	Physical manipulation	Logical destruction	Logical manipulation	Insider	Conventional weapons	Non-conventional weapons	Hand or power tools	Malicious transmitters	Software tools	Monetary means
State	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Network	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Company	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Individual	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Economic gain					■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Political power			x	x	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Market power				x	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Idiosyncratic interest	x	x	x		■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Physical destruction			x		x		x		■	■	■	■	■	■	■	■	■	■	■
Physical manipulation									■	■	■	■	■	■	■	■	■	■	■
Logical destruction					x		x		■	■	■	■	■	■	■	■	■	■	■
Logical manipulation									■	■	■	■	■	■	■	■	■	■	■
Insider				x				x	■	■	■	■	■	■	■	■	■	■	■
Conventional weapons			x								x	x	x	■	■	■	■	■	■
Non-conventional weapons			x	x	x		x	x		x	x	x	x	■	■	■	■	■	■
Hand or power tools											x	x	x	■	■	■	■	■	■
Malicious transmitters									x				x	■	■	■	■	■	■
Software tools									x	x			x	■	■	■	■	■	■
Monetary means				x				x	x	x	x	x		■	■	■	■	■	■

A.3 Outcome Matrix – Intentional Acts

State	Economic gain	Physical manipulation	Conventional weapons
State	Economic gain	Physical manipulation	Hand or power tools
State	Economic gain	Physical manipulation	Malicious transmitters
State	Economic gain	Logical manipulation	Malicious transmitters
State	Economic gain	Logical manipulation	Software tools
State	Economic gain	Insider	Monetary means
State	Political power	Physical destruction	Conventional weapons
State	Political power	Physical destruction	Non-conventional weapons
State	Political power	Physical destruction	Hand or power tools
State	Political power	Physical manipulation	Conventional weapons
State	Political power	Physical manipulation	Hand or power tools
State	Political power	Physical manipulation	Malicious transmitters
State	Political power	Logical destruction	Malicious transmitters
State	Political power	Logical destruction	Software tools
State	Political power	Logical manipulation	Malicious transmitters
State	Political power	Logical manipulation	Software tools
State	Political power	Insider	Monetary means
State	Market power	Physical manipulation	Conventional weapons
State	Market power	Physical manipulation	Hand or power tools
State	Market power	Physical manipulation	Malicious transmitters
State	Market power	Logical manipulation	Malicious transmitters
State	Market power	Logical manipulation	Software tools
State	Market power	Insider	Monetary means
Network	Economic gain	Physical manipulation	Conventional weapons
Network	Economic gain	Physical manipulation	Hand or power tools
Network	Economic gain	Physical manipulation	Malicious transmitters
Network	Economic gain	Logical manipulation	Malicious transmitters
Network	Economic gain	Logical manipulation	Software tools
Network	Economic gain	Insider	Monetary means
Network	Political power	Physical destruction	Conventional weapons
Network	Political power	Physical destruction	Non-conventional weapons
Network	Political power	Physical destruction	Hand or power tools
Network	Political power	Physical manipulation	Conventional weapons
Network	Political power	Physical manipulation	Hand or power tools
Network	Political power	Physical manipulation	Malicious transmitters
Network	Political power	Logical destruction	Malicious transmitters
Network	Political power	Logical destruction	Software tools
Network	Political power	Logical manipulation	Malicious transmitters
Network	Political power	Logical manipulation	Software tools
Network	Political power	Insider	Monetary means

Network	Market power	Physical manipulation	Conventional weapons
Network	Market power	Physical manipulation	Hand or power tools
Network	Market power	Physical manipulation	Malicious transmitters
Network	Market power	Logical manipulation	Malicious transmitters
Network	Market power	Logical manipulation	Software tools
Network	Market power	Insider	Monetary means
Company	Economic gain	Physical manipulation	Hand or power tools
Company	Economic gain	Physical manipulation	Malicious transmitters
Company	Economic gain	Logical manipulation	Malicious transmitters
Company	Economic gain	Logical manipulation	Software tools
Company	Economic gain	Insider	Monetary means
Company	Market power	Physical manipulation	Hand or power tools
Company	Market power	Physical manipulation	Malicious transmitters
Company	Market power	Logical manipulation	Malicious transmitters
Company	Market power	Logical manipulation	Software tools
Company	Market power	Insider	Monetary means
Individual	Economic gain	Physical manipulation	Conventional weapons
Individual	Economic gain	Physical manipulation	Hand or power tools
Individual	Economic gain	Physical manipulation	Malicious transmitters
Individual	Economic gain	Logical manipulation	Malicious transmitters
Individual	Economic gain	Logical manipulation	Software tools
Individual	Idiosyncratic interest	Physical destruction	Conventional weapons
Individual	Idiosyncratic interest	Physical destruction	Hand or power tools
Individual	Idiosyncratic interest	Physical manipulation	Conventional weapons
Individual	Idiosyncratic interest	Physical manipulation	Hand or power tools
Individual	Idiosyncratic interest	Physical manipulation	Malicious transmitters
Individual	Idiosyncratic interest	Logical destruction	Malicious transmitters
Individual	Idiosyncratic interest	Logical destruction	Software tools
Individual	Idiosyncratic interest	Logical manipulation	Malicious transmitters
Individual	Idiosyncratic interest	Logical manipulation	Software tools

Appendix B The Completed Scenario Templates

B.1 Accident

Scenario number 1	
Accident at nearby chemical plant	
Scenario justification	
Justification: Accidents at chemical plants or accidents during transportation of CBR (chemical, biological, radioactive material) are no rare occurrence in the world. When such accidents happen, the immediate surroundings of the site can be affected. A piqlVault or production site may be placed in such an area, and exposure to these uncontrolled emissions would then be a real threat that one should be prepared for. *Purpose*: The components of the Piql Preservation Services – the Film, the Box, the Bin and the Vault – are all vulnerable to various chemicals. Some of the components are more chemically inert than the others, but chemical agents still constitute a major risk to the system. Especially the piqlFilm is vulnerable: the gelatine emulsion on the piqlFilm, as it is a protein, is highly sensitive to chemical, and also biological, threats. *Benefit*: In knowing that this can be a prominent risk, a Piql partner can take the necessary precautions, like an additional protective layer around the piqlFilm. However, these are agents that it is difficult to provide hundred per cent protection against, and it would likely be very costly. The main recommendation is to be sure to place the piqlVault at a safe distance from such a risk source, although the risk of a transportation accident is ever present.	
Scenario outline	
The scenario is set in the geographical zone South (South America). During a hot and humid day in January an accident caused by a human error at a nearby chemical plant to a piqlVault occurs. The accident is of such a scale that chlorine gas leaks uncontrollably and in a steady stream out into the atmosphere. The damage done to the industrial facility also means that it takes several hours before the leak is fixed. Unfortunately, the wind direction and speed is such that emissions of chlorine gas reach the PiqlVault. The Piql personnel in the Vault evacuate after noticing the presence of the gas. In the process to facilitate the quick evacuation, however, doors are left open, and the presence of gas does not allow personnel to return to shut them properly. Chlorine gas is thus allowed to seep unimpeded into the Vault. The piqlBox and –Film are subjected to prolonged exposure for as long as it takes the workers at the chemical plant to get control of the leak. For this time, access to the piqlVault is made impossible.	
Cause	
Type of risk (Hazard/Threat)	Hazard: Uncontrolled emissions of a highly reactive chemical agent; here chlorine gas.

Intentional (Yes/No/Both)	No.
Profile of actor (if intentional)	-
Description of cause	An accident caused by human error at a chemical plant. At room temperatures chlorine gas is a greenish-yellow toxic gas with corrosive properties. As an oxidiser, it is extremely reactive and immediately reacts with both organic and inorganic materials it comes in contact with. As chlorine is denser than air, it tends to accumulate at the bottom of poorly ventilated spaces.
Competence and resources (if intentional)	-
User/value	
User class	Public non-sensitive.
User type	Research establishment.
Value	Past records of research papers, reports and results. Their loss is damning to the establishments current work, as many works of reference are lost. This threat has to do with general location and the Piql Preservation Services components more than specific threats to the information on the film.
Location	
Location description	Geographical zone: South (South America). The continent’s topography is marked by its flat interior and mountainous area along the Western coast. The developmental level of the continent is medium and the political climate is for the most part stable. The piqlVault is situated in an urban area, with the industrial area sitting on the outskirts of the city. The scenario takes place in the present. The time period is 0-30/50 years, as the user is business non-sensitive. The scenario is also a risk for the future, so long as regulations and protective measures are unable to fully prevent such accidents from happening or prevent the gas from spreading.
Environment description	The climate zone is a humid subtropical climate. As it is summer, near the end of January, the local weather conditions are hot and humid: 32° Celsius with a relative humidity of 89 %. The level of humidity is important, as chlorine gas is reactive with water, forming hydrochloric acid when dissolved in water. The day is clear after heavy rainfall during the night, so the humidity is noticeable. There are strong, yet subtle winds from the northwest. The accident

	occurs late morning, during business hours.
Vault description	The scenario takes place while the piqlFilm is in storage in the piqlVault. The piqlVault system is placed in a storage room located on the lower floor or basement of an office building. The vault is regulated through ventilation to uphold the ISO standards governing levels of humidity and temperature, but the day is very hot and humid.
Local safety measures	All safety measures required by Piql AS are in place, see section 5.5.1 for details. Of special notice here: the slight positive air pressure maintained inside the piqlVault slows the influx of the gas some, but due to the constant position of the open door, this advantage is soon lost.
Local security measures	All security measures required by Piql AS are in place.
Consequences	
Outer building	The physical infrastructure of the building and the storage room is not affected.
Vault	The piqlVault system is not notably affected by the chlorine gas. The aluminium in the grid can react with the gas, but the effects are delayed due to a protective oxide layer on the aluminium. With the kind of concentrations that we can assume is present (not very concentrated), the piqlVault system should be safe. The placement of vault in this case adds to the damage of the scenario and the vulnerability to the film, as chlorine is heavier than air and will therefore settle in low-lying areas.
Box	The piqlBoxes, especially the ones near the bottom of the grid, as chlorine is a low-lying gas, are affected by the gas. The chemical bonds in polymer are not very strong, so the effects from the reactive gas can make the bonds break and cause the PP in the box to crack. However, the effects of chlorine gas is worse the higher the temperature and the more humidity in the air. At 20° Celsius and normal levels of humidity, the damage is almost non-existent. There need to be temperatures of 60° Celsius and large amounts of water in the air for there to be severe damage. Under these conditions the PP would be in very bad shape. More important, however, in this scenario is the fact that the piqlBox is not air-tight, which means that the corrosive gas comes in contact with the piqlFilm.
Film	The piqlFilms near the bottom of the grid are highly affected by the reactive gas. The PET of the base of the film is resistant to chlorine gas which is dry at 15° Celsius, but not resistant at 66° Celsius. When the gas is wet, however, the PET is not resistant at either temperature. That means that a sufficient level of humidity in the air can make the chlorine gas cause severe damage to the base of the piqlFilm.

	The emulsion layer of the piqlFilm, made of gelatine, will react violently with the chlorine gas. At very little exposure it will start to corrode and completely dissolve. Additional note: The gelatine will have this reaction with many chemical agents, not just chlorine gas. Exposure to chemical agents should be avoided.
Power/energy supply	The power supply is not affected by the chlorine gas.
Divergence from ISO standard	Spin-off effect of scenario cause secondary incident: When the doors are left open to facilitate the evacuation of personnel, not only is the chlorine gas allowed to enter the piqlVault; hotter and more humid air than what is allowed inside the Vault according to regulations is let in as well. However, this will not cause much damage; it is the heightened negative effect of the chlorine gas due to higher temperatures and levels of humidity that is the culprit.
Security mechanisms	
Integrity	The gelatine emulsion of the PiqlFilms exposed to the chlorine gas will completely dissolve. This entails damage beyond repair, and the data will be lost. It will longer be possible to verify the integrity of the information.
Availability	See over. The information will no longer be available to the owner.
Confidentiality	See over. Although information will no longer be accessible to the data owner, neither will they be accessible to anybody else. Confidentiality thus remains intact, as no one else can or will read the material. All the piqlFilms in the vault were, however, left without proper security regarding access control when the doors were left open and could hypothetically have been accessed by others at this time. Other circumstances (protected by the gas) made sure no unwelcome persons dared come near the piqlFilms.
Immunity (against attacks on the above mentioned)	The Piql Preservation Services is not immune to attacks on availability or integrity.
Recommendations	
Recommended protective measures	As the risk in this scenario does not represent a direct targeting of the Piql Preservation Services, and was rather a general hazard to all in the affected area, the only advice one can give is “Beware of your surroundings”. When the piqlVault is situated near an industrial area with chemical plants, exposure to chemical agents is a risk. Either the Piql partner must take the necessary precautions, for instance installing air tight doors which shut automatically, or make the executive decision to place the piqlVault elsewhere, not in a high risk occupancy. Also, particularly when it comes to heavy gases such as chlorine gas, a specific

	solution would be to place the vault in higher floors.
References	
Literature	[48] The Engineering Toolbox (n.d.), *Chemical Resistance of PolyPropylene* [49] The Engineering Toolbox (n.d.), *Chemical Resistance of Polyesters* [74] National Institute for Occupational Safety and Health (NIOSH) Education and Information Division (2011), *Chlorine: Lung Damaging Agent* [75] CAMEO Chemicals (n.d.), *Chlorine* [76] The Royal Society of Chemistry (n.d.), *Reactions of chlorine, bromine and iodine with aluminum*

B.2 Technical Error

Scenario number 2	
Technical error in electrical system	
Scenario justification	
Justification: As the chosen storage system for the Piql Preservation Services is the AutoStore® system, referred to as the piqlVault system, which is wholly automated, an electrical fire may occur. According to the supplier of this storage system, Element Logic, the likelihood of such an event occurring is low, as the piqlVault system runs on very little electricity. The risk, however, is there regardless, and including it is natural in this assessment, as one of its focus areas is the storage phase. Fire, whether it be caused by a fault in the electrical system or not, is a common occurrence, and the Piql Preservation Services should expect to be subjected to this threat during its 500 year or longer existence. *Purpose*: The components of the Piql Preservation Services – the Film, the Box, the Bin and the Vault – are all vulnerable to extreme heat and direct contact with fire. Though plastic was chosen as the material for the PiqlFilm and –Box, among other things, for its better fire resistant properties than many other storage media, none of the components are immune to the prolonged exposure to flames; They will burn with sufficient exposure. *Benefit*: All Piql partners are required to have various measures of fire protection in place. However, not all are suited for implementation in the piqlVault. Piql AS recommend an oxygen reduction suppression solution to ward of the flames, as this causes the least damage to the rest of the Piql Preservation Services. Here, we show the benefits of following this recommendation instead of a sprinkler system.	
Scenario outline	
The scenario is set in the geographical zone North (Asia). An error in an old, outdated electrical system in the building housing the piqlVault system leads to the outbreak of an electrical fire. The error causes the system to (i) shut down and (ii) sparks to ignite a fire at the top of the grid, as this is where most of the electrical components are situated. The bottom piqlBoxes are safe from the fire as long as it is not allowed to spread. The fire protection system that the building has installed, however, is a sprinkler system. While this stops the fire from spreading notably, it poses another risk to the integrity of the films, as the piqlFilms should not be exposed to water except under controlled conditions. Neither is water a positive thing to introduce in an automated system. When the sprinklers are activated, the water splashes over the top of the grid and trickles down through the grid to assemble at the bottom of the floor, rising steadily to submerge the lower piqlFilms.	
Cause	
Type of risk (Hazard/Threat)	Hazard: Technical error of electrical system causes fire.

Intentional (Yes/No/Both)	No.
Profile of actor (if intentional)	-
Description of cause	The building within which the piqlVault system is placed is an old office building. The general infrastructure (ventilation systems, water pipes and electrical system including wiring) is outdated, and especially the electrical system is due for replacement as the Piql personnel have recently experienced many problems with old fuses and poor wiring. An electrical fire is started when an overload occurs when a robot connects to a charger on top of the grid which causes a spark and a fire is ignited. Most regular fires burn with a temperature of between 600 and 1200° Celsius depending on the materials which fuel the fire.
Competence and resources (if intentional)	-
User/value	
User class	Business non-sensitive.
User type	Consulting business.
Value	Past client history. More recent client history is stored in more accessible formats as well, but the older client history is only stored with the Piql Preservation Services.
Location	
Location description	Geographical zone: North (Asia). The developmental level of many parts of the continent is medium to high, but there are pockets of less developed areas with more dilapidated buildings and lacking infrastructure. The piqlVault is situated in an urban area, yet a little outside of the city centre where standards are more modest. The scenario takes place in the present. The time period is 0-30/50 years, as the user is business non-sensitive. The scenario is also a risk for the future, so long as the risk of electrical fires is an embedded feature of the way electrical systems are set up.
Environment description	The climate zone is a humid subtropical climate. It is autumn, in the start of September. The local weather conditions are fairly hot and the humidity is normal: 27° Celsius with a relative humidity of 78 %. It is a rainy day with drizzling. The accident occurs late in the evening as a

	robot goes to charge for the night.
Vault description	The scenario takes place while the piqlFilm is in storage in the piqlVault. The piqlVault system is placed in a storage room located on the lower floor or basement of an office building. The vault is regulated through ventilation to uphold the ISO standards governing levels of humidity and temperature. The ventilation system is powered by a backup generator after the electrical system in the building causes the piqlVault system to fail.
Local safety measures	All safety measures required by Piql AS are in place, see section 5.5.1 for details. The general standard of the building, though, indicates lack of funds to uphold the safety requirements. Of special notice here: the recommendation to use an oxygen reduction suppression solution has been ignored due to cost issues and the sprinklers already installed in the building is deemed sufficient.
Local security measures	All security measures required by Piql AS are in place. The general standard of the building, though, indicates lack of funds to uphold the security regime recommended. As the user class is business non-sensitive, a high level of security does not seem necessary to the Piql partner.
Consequences	
Outer building	The physical infrastructure of the building and the storage room is not notably affected.
Vault	The operations of the piqlVault system shuts down after the spark caused the whole electrical system to fail. The backup generator cannot regenerate the power supply, as the necessary connections in the firing have been fried. The aluminium in the grid has a melting point of between 600 and 660° Celsius. The aluminium will not burn, but it will melt. However, the integrity and stability of its mechanical properties is affected at such low temperatures as around 200° Celsius, meaning that if the structure is still standing, it will be much weakened. The water released from the sprinklers, though putting out the fire and protecting the grid and robots from the fire, cause more problems for the piqlVault system, in that it causes the electronics of the system to short-circuit. Should the piqlBins need to be extracted from the grid immediately after the fire, this must be done manually, which can be done but it is a complex and time-consuming process.
Box	The piqlBoxes near the top of the grid where the fire is strongest are affected by the fire. The PP in the piqlBoxes melts at 170° Celsius. Flame temperatures in room fires can reach between 600 and 1200°

	Celsius, but wide spatial variations will be seen. PP is a material that burns easily, and it will melt fairly quickly when exposed to fire. The once hard plastic will turn into a thick, sticky mass. The water from the sprinklers will do no notable damage to plastic of the piqlBox.
Film	The piqlFilms near the top of the grid are affected by the fire. The PET in the piqlFilms has a melting temperature at approximately 260^{o} Celsius, but already at a temperature of 75° Celsius the properties of the PET will change a lot. What happens is the same as when glass is heated; it will get softer and more viscous. If the piqlBox serves to protect the Films from some of the heat, it may well be that the melting PP of the Box will damage the film where the materials come in contact. The water from the sprinklers and possibly from fire hoses, if those are needed, can also affect the films. The piqlBox should protect the piqlFilm to a certain extent, but the Box is only splash-proof, not water-proof, i.e. not air-tight, which means that water will seep into the Boxes which are submerged in water. The piqlFilms are unaffected by this so long as they are immediately rewashed and dried properly.
Power/energy supply	The power supply to the piqlVault is highly affected by the electrical fire. The electrical connections powering the piqlVault system are completely cut off, but the generator which the piqlVault is fitted with manages to keep up other functions, such as ventilation.
Divergence from ISO standard	The temperature in the storage room naturally increases rapidly once the fire breaks out as flames generate and release large amounts of heat. Once the sprinklers are turned on, the level of humidity in the storage room also rises, but not notably. The rise in temperature is the bigger problem for the piqlFilms.
Security mechanisms	
Integrity	The piqlFilms that are in close proximity to the fire will be beyond repair and the data will be lost. It will no longer be possible to verify the integrity of the information. The information on the piqlFilms that are submerged in water may be compromised if the Films cannot be dried off properly and made safe for handling. The integrity of the remaining piqlFilms is intact, as we assume the fire is put out quickly enough and the splash-proof piqlBox provide sufficient protection against the water from the sprinklers.
Availability	The availability of all the piqlFilms is compromised temporarily, as the operations of the piqlVault system are halted due to lack of electricity. Should they be needed, however, manual recovery is possible. For the piqlFilms which are damaged beyond repair by the fire, or which cannot be saved after the long exposure to water, availability is

	irrevocably compromised. For the piqlFilms which can survive the submersion in water, availability is only temporarily compromised while the Films are dried off and prepared for safe handling again.
Confidentiality	The confidentiality of all the piqlFilms remains intact, as no unauthorised personnel gained access to the piqlVault during the scenario. The exception is, of course, the fire personnel responsible for putting the fire out.
Immunity (against attacks on the above mentioned)	The Piql Preservation Services is not immune to attacks on availability or integrity.
Recommendations	
Recommended protective measures	The purpose of this scenario is to illustrate and underline the sound recommendation from Piql to use an oxygen reduction suppression solution as the fire protection mechanism in the piqlVault. The piqlFilms and the piqlVault system are better off protected with this system.
References	
Relevant literature	[77] Babrauskas, V. (1997), *Temperatures in flames and fires* [47] The Engineering Toolbox (n.d.), *Metals - Melting temperatures* [78] Elval (n.d.), *Aluminium & Fire* [79] Summers, P. T., Chen, Y., Rippe, C. M. et. al. (2015), *"Overview of aluminum alloy mechanical properties during and after fires"*

B.3 Natural Disaster: Flood

Scenario number 3	
Flood	
Scenario justification	
Justification: Floods are a regular occurrence across the globe, and a piqlVault will almost certainly be affected by one during the next 500 years. With the effects of climate change, there may be swings in weather from severe drought to severe rainfall, which will make flooding all the more prominent. As the recommended placement of piqlVaults is in lower floors or basements in areas not affected by flood risk, it is likely that these can be subjected to floods some time in the future, if the current climate forecasts persist. *Purpose*: The particular relevance this scenario serves to the assessment of the vulnerabilities of the Piql Preservation Service is the effects of prolonged exposure to unclean water. In a severe flood the piqlFilms would likely be fully submerged in very muddy and debris-filled water for hours, even days, the effects of which would be quite different than light short exposure to clean water. Some of the components of the Piql Preservation Services, particularly the Film and the Vault, are vulnerable to prolonged exposure to water. The exact effects have not been sufficiently tested, but we can safely assume that the electronics of the piqlVault system will be severely damaged, perhaps beyond repair, necessitating full replacement, and the piqlFilm, especially the gelatine, will be highly affected. *Benefit*: This scenario highlights the need to do further testing on the piqlFilm's endurance in water, specifically unclean water, so that correct measures can be taken to prepare for (almost) inevitable exposure.	
Scenario outline	
The scenario is set in the geographical zone South (Southeast Asia). An extreme flood during the rainy season severely damages the Piql Preservation Services. Due to placement of the piqlVault in the basement of an old historical and institutional building, the raging waters quickly fill the entire space and rises to 2 meters above street level. The aging building structure is unable to withstand the pressure, and water seeps. All of the piqlFilms are fully submerged in extremely filthy water for several days, as the severity of the flood prohibits access any earlier than that.	
Cause	
Type of risk (Hazard/Threat)	Hazard: Prolonged flooding of piqlVault.
Intentional (Yes/No/Both)	No.

Profile of actor (if intentional)	-
Description of cause	Abnormal amounts of rainfall in area not prone to such high levels of precipitation causes the river which runs through the city to overflow its banks. The severity of the flood causes water to cover an enormous area, including the location of the piqlVault. The raging waters consumes almost everything in its path, from mud, vegetation and rocks to debris and remnants of buildings, and also humans and animals. The flood claims several lives.
Competence and resources (if intentional)	-
User/value	
User class	Public non-sensitive.
User type	The National Supreme Court.
Value	All manner of legal documents preserved for documentational purposes. Used as important legal references to legal practice in the country, but also as historical records of the life and times in centuries past. Though the sensitivity of the information is not high in the sense that it is confidential, its value is still very high.
Location	
Location description	Geographical zone: South (Southeast Asia). Historically, the rainy season has most affected other regions in the zone, but due to climate change floods can occur elsewhere. The developmental level of many parts of the continent is medium to high. It is rising in the region where the piqlVault is situated, but it still takes a long while before the workers reach and can start to clear the piqlVault. The piqlVault is situated in an urban area with a river running through it. Though the piqlVault is situated a safe distance from the river, the overflowing water covers an enormous area. The scenario takes place in the future, 2213. The time period is 0-100/500 years, as the value is documentational records. The scenario is a risk for the present as well, but the scale and location of the flood, and thus the placement of the piqlVault, in this scenario presupposes a change in climate patterns.
Environment description	The climate zone is a humid subtropical climate. It is the rainy season, in the end of July. The local weather conditions are hot and humid: 35° Celsius with a relative humidity of 92 %.

	It is the middle of a period of heavy rain. The river has been close to breaking point the past day and finally rises higher than its banks at the same time as tunnels, sewers and drains flood. The incident occurs early morning before business hours. The Piql personnel have been evacuated, but there was no time to start evacuating material goods.
Vault description	The scenario takes place while the piqlFilm is in storage in the piqlVault. The vault is placed in the basement of the Supreme Court building, a historical institutional building. Normally the vault is regulated through ventilation to uphold the ISO standards governing levels of humidity and temperature, but the heavy rainfall of the past days has presented a challenge with regards to humidity levels.
Local safety measures	All safety measures required by Piql AS are in place, see section 5.5.1 for details. As a building housing important legal and historical documents, the Supreme Court building was constructed with the highest regard for safety measures. Yet, the floods of the future proved too powerful for the aging building, and the structure is too weak to protect from the raging waters.
Local security measures	All security measures required by Piql AS are in place.
Consequences	
Outer building	The physical infrastructure of the building and the storage room are severely affected by the force of the flowing water, but the supporting structures of the construction still stands.
Vault	The piqlVault is highly affected by the flood. Water seeps into every crack, and eventually the doors into the storage room are forced open by the force of the water streaming in. The entire piqlVault system grid is completely submerged in water, causing all electronics to fail. The raging waters strained the integrity of the grid when it first surged in, but the strength of the aluminium and the tightly stacked bins enables it to remain upright.
Box	As the piqlVault system grid remains upright, the piqlBoxes are not subjected to jolts or drops. Neither are the piqlBoxes severely damaged by the water, yet the exposure to filthy water forces the Piql personnel to replace them, as their structural integrity has been compromised and their longevity can no longer be guaranteed. More important, however, is the fact that the piqlBox is not air-tight or water-proof, which means that the filthy water will seep in and come in contact with the piqlFilm.

Film	As the piqlBoxes are not water-proof, the piqlFilms are subjected to prolonged exposure to extremely filthy water full of mud, debris and decaying organic material. As mentioned, the exact effects are not clear, but we can safely assume that neither the polyester nor the gelatine emulsion on the piqlFilm will hold up long under these conditions. The gelatine would likely dissolve, and all of the piqlFilms would be damaged beyond repair.
Power/energy supply	Along with the rest of the city, the power supply to the piqlVault is cut off during the course of the flood.
Divergence from ISO standard	Neither the temperature, nor the humidity levels are upheld, as the power supply to keep the ventilation system running is cut. That, however, makes no difference once water fills the entire space of the storage room. The change in temperature and relative humidity will not cause much damage; the filthy water will.
Security mechanisms	
Integrity	The gelatine emulsion of the PiqlFilms exposed to the filthy water will almost certainly completely dissolve. This entails damage beyond repair, and the data will be lost. It will no longer be possible to verify the integrity of the information.
Availability	See over. The information will no longer be available to the owner once it becomes evident the information on the piqlFilms cannot be saved.
Confidentiality	See over. Although information will no longer be accessible to the data owner, neither will it be accessible to anybody else. Confidentiality thus remains intact, as no one else can or will read the material. All the piqlFilms in the vault were left without proper security regarding access control when the doors were forced open by the pressure of the water and could hypothetically have been accessed by others at this time. Due to circumstances outside of human control, however, the films remained inaccessible and thus confidential.
Immunity (against attacks on the above mentioned)	The Piql Preservation Services is not immune to attacks on availability or integrity.
Recommendations	
Recommended protective measures	The piqlVault is more vulnerable to the effects of flooding when it is placed in the lower floors of a building, hence the recommendation is to place it higher up in areas prone to flooding. As this scenario has illustrated that one cannot in the future always know whether one is in an area prone to flooding or not, additional measures should be in place. These could include a sealed bag around the piqlBox. Another measure

	is to always keep backup copies of the piqlFilms at several places, which is a regulation in force today.
References	
Relevant literature	[80] FloodList (n.d.), *Asia*

B.4 Natural Disaster: Forest Fire

Scenario number 4	
Forest fire	
Scenario justification	
Justification: Forest fires are a regular occurrence across the globe, and a piqlVault will most likely be placed in the path of one during the next 500 years. In fact, with the effects of climate change, there may be swings in weather from severe drought to severe rainfall. Such extreme droughts increase the chance of forest fires. Additionally, urbanisation and population growth will strain the current boundaries of cities around the world, and it is possible that more and more construction will take place near a forest line, in the urban/rural interface and also in wooded areas. These two factors combined mean that the Piql Preservation Services may be more exposed to the dangers of forest fires in the future, and that is not to say that it does not constitute a problem even today. The potential damages to the Piql Preservation Services are high, as it requires the swift extinction of a fire to avoid the information stored being lost. *Purpose*: The components of the Piql Preservation Services – the Film, the Box, the Bin and the Vault – are all vulnerable to extreme heat and direct contact with fire. Though plastic was chosen as the material for the PiqlFilm and –Box, among other things, for its better fire resistant properties than many other storage media, none of the components are immune to the prolonged exposure to flames; They will burn with sufficient exposure. The longer the fire is allowed to burn, the higher the risk of destruction of the piqlFilms, and a forest fire is much harder to control and put out than room fires. *Benefit*: All Piql partners are required to have various measures of fire protection in place. They must make sure that these are enough to hold off even a prolonged fire.	
Scenario outline	
The scenario is set in the geographical zone North (Europe). After a period of excessive heat and drought, the piqlVault, located in a building situated in the urban/rural interface, is caught in a fierce forest fire which is particularly hard to extinguish. The local fire department is unable to get control of the fire and it is allowed to rage in the vicinity for a fortnight. During this period, the forest fire consumes parts of the building. Even when the building is no longer on fire, the fire department will not allow reentry due to the dangers of the forest fire reaching the building again.	
Cause	
Type of risk (Hazard/Threat)	Hazard: Unmanageable forest fire engulfs the piqlVault.
Intentional (Yes/No/Both)	No.

Profile of actor (if intentional)	-
Description of cause	A forest fire is an uncontrolled fire occurring in nature. These are more difficult to get under control than room fires and therefore last for longer periods of time. The urban/rural interface is a location where buildings are more vulnerable to forest fires than in a city, due to the close proximity to the wooded areas.
Competence and resources (if intentional)	-
User/value	
User class	Public non-sensitive.
User type	The National Archive.
Value	Various historically and culturally important documents preserved for documentational purposes, stored for the preservation of the collective cultural memories of a society and important records of past times. Though the sensitivity of the information is not high in the sense that it is confidential, its value is still very high. The rarest artefacts are stored in a mountain hall, but many documents are also stored aboveground.
Location	
Location description	Geographical zone: North (Northern Europe). The continent's landscape is marked by mountainous areas and flat, wide expanses and river valleys with much vegetation. The developmental level of the continent is high and the political climate is stable. The piqlVault is situated in an urban area, though in the urban/rural interface right on the edge of a forested area. The scenario takes place in the future, 2158. The time period is 0-100/500 years, as the value is documentational records. The scenario is a risk for the present as well, but the scale and ferocity of the forest fire in this scenario presupposes a change in climate patterns.
Environment description	The climate zone is temperate. It is summer, in the middle of August, and the local weather conditions are hot and dry: 36° Celsius with a relative humidity of 41 %. These abnormally high temperature levels and low relative humidity levels have persisted for weeks. The wooded areas surrounding the city are extremely dry, and the government have issued statements urging hikers to beware the dangers of causing a forest fire. One such hiker is unobservant and starts a fire which quickly gets out of control. The

	incident occurs in the middle of the working day, but it takes several hours before the fire department alerts the Piql personnel and orders them to evacuate as quickly as possible. Before they leave, they activate the oxygen reduction suppression mechanism inside the piqlVault.
Vault description	The scenario takes place while the piqlFilm is in storage in the piqlVault. The vault is placed in the lower floors of the National Archive building. Underneath the building there is a mountain repository with the highly rare documents, but for the purposes of this scenario we analyse the piqlFilms in the building aboveground, as the films placed in the mountain hall would be completely safe from the fire and extreme temperatures. The vault is regulated through ventilation to uphold the ISO standards governing levels of humidity and temperature, but the day itself is very hot.
Local safety measures	All safety measures required by Piql AS are in place, see section 5.5.1 for details. Of special notice here: the oxygen reduction suppression solution is in place and activated during the incident, but there is a limited supply of the oxygen restricting gas to suffocate the fire.
Local security measures	All security measures required by Piql AS are in place.
Consequences	
Outer building	The physical infrastructure of the building and the storage room are severely affected by the fire, though there are some remedying factors which help the situation. Due to the building's location on the outskirts of the forest, it takes some time for the fire to spread out to the forest edge. Once it does, however, the fire spreads quickly from the vegetation to the building structure. Another positive thing about the location of the building is that it is more easily accessible to the fire department than it would have been had it been located deeper into the forest. Additionally, the construction is made of cement/brick, so it does not burn to the ground.
Vault	The parts of the piqlVault system which are touched by fire are highly affected by increase in temperature and the flames themselves. As the piqlVault is placed on the lower floors of the National Archive, it is easily accessible to the fire. Even though the piqlVault is equipped with the oxygen reduction suppression mechanism, the forest fire persists to the point when the supply of the oxygen restricting gas is depleted. Once the fire is allowed to spread to the piqlVault, and the grid is subjected to the flames, the structural integrity of the aluminium grid collapses completely, as the exposure to the fire is prolonged. The aluminium in the grid has a melting point of between 600 and 660° Celsius. The aluminium will not burn, but it will melt. However, this

	does not cause the entire structure to collapse, as the stacking of the piqlBins help to keep it upright.
Box	The piqlBoxes that are in contact with the flames and in their near proximity will be severely affected by the fire. The PP in the piqlBoxes has a melting temperature of 170° Celsius, and regular room fires can reach between 600 and 1200° Celsius. The PP will therefore melt fairly quickly, especially when exposed to fire for a longer period of time as the extreme temperatures are sustained. The once hard plastic will turn into a thick, sticky mass. If the piqlBoxes come in contact with the melted aluminium of the grid, that will cause more damage as well. The piqlBoxes which do not melt have still been subjected to extreme temperatures. They will need replacing, as their structural integrity has been compromised and their longevity can no longer be guaranteed.
Film	The piqlFilms that are in contact with the flames and in their near proximity will be severely affected by the fire. The PET in the piqlFilms has a melting temperature at approximately 260^{o} Celsius, but already at a temperature of 75° Celsius the properties of the PET will change a lot. What happens is the same as when glass is heated; it will get softer and more viscous. If the piqlBox serves to protect the Films from some of the heat, it may well be that the melting PP of the Box will damage the film where the materials come in contact. The piqlFilms which do not melt have still been subjected to extreme temperatures. This will also affect the readability of the piqlFilm, as everything will get blurred.
Power/energy supply	The forest fire causes a general power outage in the area near the piqlVault, but the generator which the piqlVault is fitted with manages to keep up other functions, such as ventilation. When the fire reaches the building, however, the electrical wiring short-circuits and all power supply is lost.
Divergence from ISO standard	The temperature in the storage room naturally increases rapidly once the fire breaks out as flames generate and release large amounts of heat. The flames, of course, do the most damage, but the rise in temperature in the confined space will increase the negative effect on the remaining piqlFilms.
Security mechanisms	
Integrity	The piqlFilms that are in close proximity to the fire will be beyond repair and the data will be lost. It will no longer be possible to verify the integrity of the information. The information on the piqlFilms that are subjected to the extreme heat may blur, depending on the proximity to the fire source. The damage, however, would have been far greater without the oxygen

	reduction suppression mechanism, as that would have allowed the fire to rage for a longer period. The integrity of many piqlFilms is saved by the presence of this solution.
Availability	For the piqlFilms which are damaged beyond repair by the fire, or which have blurred beyond visibility due to the high temperatures, availability is irrevocably compromised. The damage, however, would have been far greater without the oxygen reduction suppression mechanism, as that would have allowed the fire to rage for a longer period. The availability of many piqlFilms is saved by the presence of this solution. The availability of the remaining piqlFilms is compromised temporarily, as the structural stability of the piqlVault system grid cannot support the robots needed for retrieval of the piqlBins. Neither is the mechanism for manual recovery possible to use. The surviving piqlBins must be extracted from the remains of the charred piqlVault system one by one by hand.
Confidentiality	The confidentiality of all the piqlFilms remains intact, as no unauthorised personnel gained access to the piqlVault during the scenario. The exception is, of course, the fire personnel responsible for putting the fire out. The confidentiality of the information was threatened for a time, as the structural integrity of the building had been compromised and as such perimeter security could not be guaranteed, but the dangerous environment served as security in itself.
Immunity (against attacks on the above mentioned)	The Piql Preservation Services is not immune to attacks on integrity or availability.
Recommendations	
Recommended protective measures	The recommendation from Piql AS to use an oxygen reduction suppression solution such as the fire protection mechanism in the piqlVault is regarded as the best one. Making sure the supply of the oxygen restricting gas is such that it can withstand prolonged fires is important.
References	
Relevant literature	[81] Gabbert, B. (2011), *At what temperature does a forest fire burn?* [82] Kriseinfo.no (n.d.), *What is a forest fire?*

B.5 Natural Disaster: Earthquake

<table>
<tr><th colspan="2">Scenario number 5</th></tr>
<tr><td colspan="2"><b>Earthquake</b></td></tr>
<tr><td colspan="2"><b>Scenario justification</b></td></tr>
<tr><td colspan="2"><i>Justification</i>: Earthquakes are a global phenomenon and they occur at regular intervals around the world. Though we can determine the regions most prone to earthquakes with a level of certainty, it is unlikely that no piqlVault will be placed in such a region. Construction techniques have come a long way in mitigating the effects of seismic tremors, yet the size and corresponding force of many earthquakes still inflict much damage even on buildings which are built using these techniques. The earthquake which caused the devastating tsunami on 26th December 2004 measured 9.1 on the Richter scale. Analysing the effects an earthquake would have on the piqlVault and the potential damage it can do to the piqlFilms is therefore necessary.
<i>Purpose</i>: None of the components of the Piql Preservation Services – the Film, the Box, the Bin and the Vault – are designed to withstand the level of physical pressure from overhead weight they are put under when pieces of concrete falls on top of them due to the tremors affecting the building they are placed in. In fact, little testing has been done to this effect. Though plastic is a strong material, it will be crushed under these circumstances.
<i>Benefits</i>: This scenario highlights the need to do further testing on the piqlFilm, -Box and -Bin regarding the kind of physical pressure it can withstand when subjected to external impacts.</td></tr>
<tr><td colspan="2"><b>Scenario outline</b></td></tr>
<tr><td colspan="2">This scenario is set in the geographical zone North (North America). An earthquake measuring 7.5 on the Richter scale hits the region in July during an extreme heat wave with temperatures often reaching above 40° Celsius. The earthquake causes the building which holds the piqlVault to shake violently, greatly damaging the building. Although the building remains standing, pieces of concrete break free from the construction and falls on top of the piqlVault system containing the piqlFilms and -Boxes, which cannot withstand that kind of pressure. Additionally, the remaining piqlFilms are exposed to higher levels of temperature and relative humidity than they should when the shift in the building's structure causes the electrical system, and thus the ventilation system, to fail. The earthquake also causes the plumbing in the walls and ceiling around the piqlVault to burst and the piqlFilms to be exposed to water. The storage room itself was damaged to such an extent that its secure doors are forced into an open position, exposing the film further to the outside environment and constituting a breach in perimeter security.</td></tr>
<tr><td colspan="2"><b>Cause</b></td></tr>
<tr><td>Type of risk (Hazard/Threat)</td><td>Hazard: Earthquake during a heat wave.</td></tr>
<tr><td>Intentional</td><td>No.</td></tr>
</table>

Profile of actor (if intentional)	-
Description of cause	Earthquakes are the result of movement of tectonic plates. It causes the ground to shake, and at worst causes the earth to open and buildings' infrastructure to collapse. It often leads to severe damage to property and serious injury and/or loss of life.
Competence and resources (if intentional)	-
User/value	
User class	Business non-sensitive.
User type	Movie and television production company.
Value	Records and copies of all past productions. These are a testament to the rich and varied history of the company, but their value is also an evidence of and memories from a celebrated time period in a society.
Location	
Location description	Geographical zone: North (North America). Parts of the region are situated on the so-called Pacific Ring of Fire, an area very prone to earthquakes due to the positioning of tectonic plates. The earthquakes are often of a considerable size. The developmental level of the continent is high and the political climate is stable. The piqlVault is situated in an urban area, in the business district in the downtown area surrounded by skyscrapers in close proximity. The scenario takes place in the present. The time period is 0-30/50 years, as the user is business non-sensitive. The scenario is also a risk for the future, so long as the construction of buildings is unable to mitigate one hundred per cent the effects of earthquakes.
Environment description	The climate zone is a subtropical climate. It is summer, in the middle of July. The local weather conditions are hot and humid: 39° Celsius with a relative humidity of 90 %. These high levels have great effect on the piqlFilm when the ventilation system stops functioning. It is a warm and humid day, as the region is in the middle of a heat wave where temperatures frequently exceed 40° Celsius. The incident takes place during the last morning office hours.
Vault description	The scenario takes place while the piqlFilm is in storage in the piqlVault. The piqlVault system is placed in a storage room located on the 32nd floor of an office building (skyscraper).

	The vault is regulated through ventilation to uphold the ISO standards governing levels of humidity and temperature, but the day itself is very hot and humid.
Local safety measures	All safety measures required by Piql AS are in place, see section 5.5.1 for details. Of special notice here: as this area is very prone to earthquakes, the building has been constructed following all national regulations regarding seismic mitigation.
Local security measures	All security measures required by Piql AS are in place. Even though the user class is business non-sensitive, the company is a powerful one with many resources at its disposal and a reputation to uphold.
Consequences	
Outer building	The physical infrastructure of the building and the storage room is highly affected. The scale and force of the earthquake was such that it surpassed the seismic mitigation measures, though these did prohibit the building from collapsing.
Vault	The infrastructure of the storage room shifts so that the doors to the room are left in an open position, letting hot and humid air into the vault during the heat wave. This allows uncontrolled access to the piqlFilms as well. As the ventilation system has shut down, the negative effects of the increase in temperature and humidity are worsened. Neither is the connection to the backup generator working. The stability of the piqlVault system grid, with the combined strength of the structure and the tightly stacked piqlBins, enables it to remain upright during the earthquake, though the grid is noticeably broken in places. However, the earthquake also causes large pieces of armoured concrete from the ceiling to fall on top of the grid, crashing through the top piqlBins, -Boxes and -Films. Water from the bursting pipes sprinkles over parts of the grid and the robots, whose electronics short-circuit when they come in contact with the water. This, however, does little to change the overall functionality of the piqlVault system, as the damages described above will require a full replacement of the system regardless of the water damage.
Box	As the grid remains upright, the piqlBoxes are not strewn across the floor, but rather remain in the piqlBins and receive some protection from the water streaming from the busted water pipes. Small amounts of clean water do little to affect the piqlBox. This means little to the piqlBoxes near the top of the grid which are crushed by the falling concrete slabs. These, and their contents, are completely destroyed by the impact. However, it is difficult to say what the situation is for the lower piqlBoxes, the ones which survived the initial impact from the concrete slabs, but which now have to withstand the increased physical pressure from the weight of the slabs. There has not been performed any testing on this, though the

	piqlBox is intended to protect its contents from an impact of 5 Joule. It should be noted that this is quite low, and even if the piqlBoxes do hold up to this standard, it would not guarantee their endurance under the physical pressure described here. With regards to the exposure to higher levels of temperature and humidity, the problems really only makes themselves known when the exposure is long-term. Humidity is less of a problem, but increased temperature over longer periods of time will soften and cause deformation of the piqlBox. The additional static load of the concrete slabs will also cause the deformation to increase. However, it should be noted that while the piqlBox can withstand such increases in temperature for a time, the piqlFilm is much more vulnerable both in terms of temperature level and the duration of exposure.
Film	The majority of the piqlFilms lay secure in their piqlBoxes, as the grid did not fall or collapse. The piqlFilms inside the piqlBoxes which were struck by the concrete slabs, however, are crushed beyond repair. As is the case with the piqlBoxes, it is difficult to say how the piqlFilms which survived the initial impact from the concrete slabs fare. The properties of the piqlFilms when it comes to withstanding physical pressure is not known, neither is there a standard they should adhere to on this point. All that is for certain is that there is an advantage in the way that piqlFilms are tightly rolled into a coil. This way they are able to withstand more physical pressure than when uncoiled. The remaining piqlFilms are exposed to temperatures of 35-40° Celsius and relative humidity of 90 %, as the ventilation system shut down and warm and humid air is let into the vault. The piqlFilms must remain under these conditions until the building is made safe to enter. Considering the damage the earthquake has done to the city at large, and the priorities of the repair workers, this takes at least 48 hours. Calculations show an increase of 0.02-0.1° Celsius per hour when the ventilation system fails. One can only imagine what it is like when the local weather conditions are as extreme as this as well. When the film is exposed to higher temperatures and humidity levels than they should it can affect readability as the information on the films floats out and gets blurred.
Power/energy supply	Damage to electrical wiring and water pipes. Loss of all electrical power, cutting all ventilation and affecting all security and general monitoring systems. The backup generators were affected by the tremors as well.
Divergence from ISO standard	The power supply to the piqlVault is completely cut off by the earthquake. Neither is the backup generator able to bring the power supply back up. The loss of ideal storage conditions is worsened when warm and humid air is allowed into the vault through open doors and cracks in the infrastructure of the storage room.

Security mechanisms	
Integrity	The piqlFilms which were crushed by the falling concrete slabs are damaged beyond repair. It will longer be possible to verify the integrity of the information stored on these piqlFilms. The integrity of the piqlFilms subjected to the additional physical pressure of the slabs may be compromised if these too are crushed. For the remaining piqlFilms, the loss in ideal storage conditions may cause the information to blur so that it cannot be read back. If that is the case, integrity is lost for these piqlFilms as well.
Availability	Availability is compromised for all the piqlFilms for some time, as the Piql personnel are unable to access the vault due to the unsafe stability of the structure of the office building. The availability of the piqlFilms which are crushed and the piqlFilm which potentially succumb to the pressure of the slabs is permanently compromised. For the piqlFilms which have blurred beyond visibility due to the high temperature and humidity, availability is irrevocably compromised. If it turns out some of the piqlFilms can be made readable again, then their availability is compromised only temporarily.
Confidentiality	The confidentiality of all the piqlFilms remains intact, as no unauthorised personnel gained access to the piqlVault during the scenario. The information on the piqlFilms which were crushed by the concrete slabs will remain forever confidential. The confidentiality of the remaining piqlFilm was threatened for a time, as the structural integrity of the building had been compromised and as such perimeter security could not be guaranteed, but the dangerous environment served as security in itself. The films remained inaccessible and thus confidential.
Immunity (against attacks on the above mentioned)	The Piql Preservation Services is not immune to attacks on availability or integrity.
Recommendations	
Recommended protective measures	A piqlVault is more vulnerable to the effects of an earthquake when it is placed in the upper floors of a building. In an area prone to earthquakes (but not to floods), place the piqlVault in lower floors or in the basement. Additionally, more testing on the piqlBox is recommended to understand what is needed to reinforce the primary packaging of the piqlFilm to withstand more pressure from external impacts and thus better protect the piqlFilm.
References	
Relevant literature	

B.6 Crime: Theft

Scenario number 6

Theft/criminality

Scenario justification

Justification: Theft is one of the most relevant threats that the Piql Preservation Services faces. Depending on the sensitivity and value of the information stored on the piqlFilm and the capacity and intentions of the threat actors, they may attempt to steal the piqlFilms from inside the piqlVault. If the threat actor can enlist the help of an insider, a Piql operator prone to criminal behaviour, the greater the danger to the security of the piqlFilm is. This scenario can be valid for all sectors and all nations, and as such is an important one.

Purpose: In one (future) context or another, the piqlFilms are a likely target for theft. Such a deliberate attack on the Piql Preservation Services is perhaps the greatest challenge it will face. Here, the threat actor will specifically target and make informed decisions on how to breach the security parameters surrounding the piqlVault, unlike when the Piql system is subject to an accident or it is collateral damage in a separate event. The importance of proper protection to prevent and/or obstruct such attacks cannot be stressed enough.

Benefit: To highlight the importance of securing the Piql Preservation Services against deliberate threats both external and internal.

Scenario outline

The scenario is set in the geographical zone Middle (Middle East). In a future setting there is a worldwide scarcity of oil and no alternative energy source. The demand for oil is sky high, and so are its prices. With this as the main motivation a major rival oil company X steals oil well analyses from the oil company Y which uses the Piql system for their archival needs. These are analyses from several “dry” oil wells that have been drilled in one of company Y’s oil fields since early 2020. The analyses have been done using a new technology applied to old seismic data which can show that the “dry” oil wells are not dry at all. Having this technology means that the oil company Y can buy “dry” oil wells at low costs and still make a profit. Being the only oil company on the market with this knowledge gives them a great advantage. The rival oil company X naturally wants to get their hands on this new method of oil well analysis. Such is their desire for the information that the actor decides to bribe a Piql operator working at company Y’s headquarters. The insider is a high level operator and has complete access to the EWMS in the piqlVault system. The operator easily orders the pickup of the relevant piqlFilms and simply removes them from the facility. The transaction is logged and the operator is later revealed to be the culprit, but the bribe was of such a substantial size that the operator has already left the country to start a new life elsewhere. Regardless, the damage has already been done: oil company Y has lost its competitive advantage.

Cause	
Type of risk (Hazard/Threat)	Threat: Theft of trade secrets on piqlFilm committed by insider on behalf of someone standing to gain financially from the information obtained.
Intentional (Yes/No/Both)	Yes.
Profile of actor (if intentional)	The rival oil company X is one of the biggest in the world. It has shown in the past that it is without scruples and willing to bend the rules to reach its objectives. Moreover, as it is state-owned, it has huge resources at its disposal.
Description of cause	Due to the scarcity of oil and accompanying high prices, the rival oil company X is motivated to go to extreme measures to get a bigger market share. In acquiring the oil well data in question, where the new method of oil well analysis is used, the rival company X gains new insight into which oil wells on the depleted market have the potential for further exploration, and the financial reward could be considerable in the current market. A second, less vital, aspect is how the rival oil company X also gets access to information on how oil company Y conducts oil well analyses generally, and is able to compare the efficiency of their respective methods to perhaps make a change in the future. Oil company X resorts to bribing a Piql operator. Said operator suffers from gambling addiction and is in grave financial debt, and so is open to bribes.
Competence and resources (if intentional)	As one of the major state-owned oil companies of the world, the rival oil company X has the financial resources available to bribe the insider with large sums of money. It also has a lack of scruples to engage in such acts of corruption.
User/value	
User class	Business sensitive.
User type	Oil and gas sector. Major oil company Y.
Value	Trade secrets, specifically oil well analyses of “dry” wells which details how new technology can be applied to old seismic data to show if an oil well is profitable after all. The information is potentially worth millions of USD. Highly company confidential. Even if the information is eventually recovered or the company have copies, the loss of the company’s market position due to loss of confidentiality is very damaging.

Location	
Location description	Geographical zone: Middle (Middle East). The region was rich in oil resources, with many oil fields which can be potential lucrative sites for oil drilling again. The developmental level is not very high, and construction techniques are not very modern or advanced. The piqlVault is situated in an urban area, right in the city centre. The scenario takes place in the future, 2157, as it presupposes an imagined situation in which oil is scarce, but no alternative energy source has yet been discovered. The time period is 0-30/50 years, as the user is business sensitive. The scenario is also a risk in the present, so long as the Piql Preservation Services store information which others are willing to go to great lengths to gain access to.
Environment description	The climate zone is hot desert with very little precipitation. It is spring, the beginning of May. The local weather conditions are fairly hot and dry: 25° Celsius with a relative humidity of 38 %. The incident occurs late afternoon, when there are fewer people in the piqlVault than during the busy hours of midday.
Vault description	The scenario takes place while the piqlFilm is in storage in the piqlVault. The piqlVault system is placed in a storage room located in basement of an office building. The vault is regulated through ventilation to uphold the ISO standards governing levels of humidity and temperature.
Local safety measures	All safety measures required by Piql AS are in place, see section 5.5.1 for details. However, the developmental level is not the highest, which is reflected in the sophistication level of the implementation.
Local security measures	All security measures required by Piql AS are in place.
Consequences	
Outer building	The physical infrastructure of the building and the storage room is not affected.
Vault	The structural integrity of the piqlVault system is not affected during the theft. However, the piqlVault system is the part of the Piql Preservation Services which is breached. A high level employee with complete login access to the system is able to use the EWMS to retrieve the relevant piqlFilms. Though the EWMS only stores the reel IDs of the piqlFilms, as this was an insider theft, the operator already knew which ID number corresponded to the piqlFilms of interest to the rival oil company X. The transaction is logged, as all transactions are in the EWMS, which ultimately leads to the capture of the operator in question. Yet, as there

	is no continuous surveillance in the system to catch irregular transactions, it is not brought to light soon enough, and the information is already in the wrong hands. As the insider is a high level operator, and as such enjoys a certain level of respect from his/her co-workers, the operator is not challenged when picking up the piqlFilm from the operator port, nor do the other employees react when he/she leaves the facility with the films.
Box	The piqlBox is not affected during the theft.
Film	The piqlFilms in question are not damaged, but they are removed without authorised permission.
Power/energy supply	The power supply is not affected during the theft.
Divergence from ISO standard	The storage conditions of the Piql Preservation Services are not affected during the theft.
Security mechanisms	
Integrity	As the piqlFilms are not damaged during the incident, the data is not lost in the sense that it is altered. The integrity of the piqlFilms thus remains intact.
Availability	The availability of the piqlFilms is compromised, as the information stored on them is no longer accessible to the data owner.
Confidentiality	Most importantly for the data owner, the confidentiality of the information stored on the PiqlFilms was irrevocably compromised, as another actor who absolutely should not have had access to its contents did gain access. The loss of confidentiality also resulted in grave financial consequences for the data owner.
Immunity (against attacks on the above mentioned)	The Piql Preservation Services is not immune to attacks on availability or confidentiality.
Recommendations	
Recommended protective measures	To mitigate the threat of the insider, the following guidelines are advised: 1. Make sure sound procedures for vetting of potential employees are in place during hiring processes. These can include full security clearance or criminal record and credit check depending on sector. 2. Perform such checks at regular intervals, not just at the start of the employment, to ascertain whether any change in circumstance has come about which can have a negative effect on the way an

	employee conducts him- or herself at work. 3. Implement a system where piqlFilms cannot be removed from the grid without being signed out by a second Piql operator. 4. Implement a control system which does not allow piqlFilms to leave the facility unless authorised by two or more authorised personnel.
References	
Relevant literature	[83] Lundin Norway AS (n.d.), *Letestrategi*

B.7 Crime: Organised Crime

Scenario number 7	
Organised crime	
Scenario justification	
Justification: As with theft done by an individual, depending on the sensitivity and value of the information stored on the piqlFilms in question, a more organised form of crime is likely to target the Piql Preservation Services. This can include mafia groups, drug cartels or human traffickers. The information on the PiqlFilm could be of such a nature that the networks in question can profit directly from their knowledge thereof; they can sell it to a third party (on order); or they can use the information to extort other individuals. Whatever the motivation, this is a risk the Piql Preservation Services needs to be aware of. *Purpose*: Regardless of their contents, the piqlFilms will always be much more vulnerable when they are out in the open, i.e. when they are not in a controlled environment such as the production site and the storage facility. The transportations phase between the two is thus a time when the piqlFilms are especially vulnerable. If the information stored in addition is such that someone can stand to profit from their possession, then theft during this phase is a real risk. *Benefit*: This scenario serves to illustrate just such a scenario: One where a group with knowledge of the piqlFilms' contents and the means to pull off a major heist, who has studied the operations of the Piql PS and identified the transportation phase as the most likely point of success. To arrange for continuous security is therefore important, not just while the piqlFilms are produced or while they are in storage.	
Scenario outline	
The scenario is set in the geographical zone South (South America). While finished piqlFilms containing personal data, including social security numbers, are transported from the production site to the designated storage facility, the truck is robbed by a street gang with connections to a drug cartel. The truck makes its way along its route without incident, but when it stops at the delivery site to unload its contents, it is overrun by assailants. A gang of four masked persons overpowers the driver and the additional guard. They are forced, on pain of death, to give up the code to the truck's loading area. The gang makes away with the piqlFilms, with the intent to sell them to a potential buyer who had contacted them with an interest in ID theft. Upon receiving thus lucrative offer, the group starts to meticulously plan their attack. They do surveillance on the Piql partner to learn their routines and find weaknesses, which leads them to learn when and how to strike in order to succeed in their theft.	
Cause	
Type of risk (Hazard/Threat)	Threat: Theft of personal data on piqlFilm committed by a street gang with connections to a drug cartel with the intent to sell to a third party.

Intentional (Yes/No/Both)	Yes.
Profile of actor (if intentional)	The drug cartel is based in South America. Their modus operandi involves ruthless tactics and a “kill first, ask questions later” mentality. They believe there is strength in numbers and a great deal of firepower. They must portray an image of strength and power to remain on top in a harsh reality where other groups are ready to take the top spot at a moment’s notice.
Description of cause	The drug cartel gets most of its revenue from the production and sale of cocaine, but it is always looking for new opportunities of profit-making. These sorts of operations are their source of income. Hence, when the cartel is contacted by a third party interested in personal data to use in his/her organisation of ID theft, the cartel jumps at the opportunity. After a brief look at the operations of the Piql partner to assess the difficulty of the mission, they decide to take the job. The motivation is the short-term financial reward, as well as the possibility to expand their outfit permanently to include ID theft.
Competence and resources (if intentional)	As one of the most powerful gangs is the area, with a good foothold in and much support from society, the cartel has access to all the relevant material they need, including weapons, etc. The heist took some planning, which for this organised crime syndicate, was an easy matter as they can work as a team and assign tasks within the group.
User/value	
User class	Public sensitive.
User type	Public registry of personal data.
Value	Personal data, including social security numbers. The dissemination of such information is strictly regulated, due to its vulnerability of abuse and how it can cause complications for the individuals who are targeted.
Location	
Location description	Geographical zone: South (South America). The region has historically been plagued by gang activity, especially related to the production and sale of narcotics, as the continent’s climate and topography provide good conditions for growing these plants. Though the developmental level of the continent is medium and the political climate is for the most part stable, some regions, particularly urban areas, see a lot more violence, poverty and destitution than others. Both the production site and the storage facility are centrally located in a major city, right in the city centre. The scenario takes place in the present. The time period is 0-30/50 years,

	as the value is time-sensitive, i.e. only for as long as the persons whose identities are stolen are alive. The scenario is also a risk for the future, so long as a profit can be made from ID theft.
Environment description	The climate zone is a humid subtropical climate. As it is summer, near the end of January, the local weather conditions are hot and humid: 32° Celsius with a relative humidity of 89 %. The incident occurs in the middle of the day, not during the morning or afternoon rush. This suits the drug cartel well, as they wouldn’t prefer to attack the truck when there are lots of people around.
Transport description	The scenario takes place during transportation of the piqlFilm. The setting is therefore the armoured truck, a veritable vault on wheels.
Local safety measures	As the incident takes place during transportation, this is not relevant.
Local security measures	The elements of the security regime defined for the purposes of the assessment are in place.
Consequences	
Outer building	As the incident takes place during transportation, the effect on the infrastructure of the building housing the Piql Preservation Services is not relevant.
Transport	Here: The armoured truck. The structural integrity of the truck is not damaged, but the integrity of the security regime is compromised when the guards are unable to fend off the assailants. The guards are forced at gunpoint to first unlock the holding area and then give up the PIN code that unlocks the safe, enabling the assailants to get away with the piqlFilms in question.
Box	The piqlBox is not affected during the theft.
Film	The piqlFilms in question are not damaged, but they are removed without authorised permission.
Power/energy supply	As the incident takes place during transportation, the effect on the power supply to the building housing the Piql Preservation Services is not relevant.
Divergence from ISO standard	As the incident takes place during transportation, the storage conditions in the piqlVault are not relevant.

Security mechanisms	
Integrity	As the piqlFilms are not damaged during the incident, the data, though stolen, is not lost in the sense that it is altered. The integrity of the piqlFilms remains intact.
Availability	The availability of the piqlFilms is compromised, as the information stored on them is no longer accessible to the data owner.
Confidentiality	Most importantly for the data owner, the confidentiality of the information stored on the PiqlFilms was irrevocably compromised, as another actor who absolutely should not have had access to its contents did gain access. The loss of confidentiality comes at a cost to a great many people whose identities are now at the risk of being misused.
Immunity (against attacks on the above mentioned)	The Piql Preservation Services is not immune to attacks on availability and confidentiality.
Recommendations	
Recommended protective measures	It is difficult to give a general recommendation which can be applied to all situations involving theft during transportation. There is the general need to assess ones surroundings and implement the security strategy accordingly. In the scenario here, the transportation takes place in an area where there is a lot of gang activity. Here, it would perhaps be prudent to raise the level of security. Another more general recommendation can be changing the routes of the transportation from day to day so as to take away the assailants ability to plan precisely where to stage the attack.
References	
Relevant literature	[84] Security Incorporated Corp. (n.d.), *Armored Transport Service*

B.8 Sabotage

Scenario number 8	
Sabotage	
Scenario justification	
Justification: Sabotage is a real vulnerability to any system. This could be a wire being cut, a control panel being smashed or a microchip being dislodged in a vital machine. The same vulnerability exits in the Piql Preservation Services. *Purpose*: The purpose of this scenario is to stress the vulnerability of the Piql system to sabotage, be it sabotage against the structural integrity of the building housing the storage facility or production site, against the piqlVault system, against the necessary machines in the production process, or against the piqlFilm directly. This particular case is a case of logical sabotage which takes place on the Piql computer which receives and processes the client data before writing. *Benefit*: This scenario seeks to highlight the importance of protective measures against acts of sabotage, particularly where it comes to IT security. Though the information stored with the Piql Preservation Services is immune to logical threats for most of its existence, as it is an offline medium, the risks are still present during production.	
Scenario outline	
The scenario is set in the geographical zone South (Southern Africa). A state actor, state X, is able to break through the computer security defences of the Piql partner and performs logical sabotage on the client information – important diplomatic correspondence. As a state actor, state X has formidable resources and skills where it comes to accessing other computer systems without authorisation. Due to the relatively strong security mechanisms put in place by Piql AS, only skilful hackers with a big support system are able to perform the kind of sabotage we are outlining here: logically tampering with the printing process so that the finished piqlFilm is missing vital information that the data owner sent in. This is only possible if state X is able to plant malware on the Piql (reception) computer which uses the physical link between that computer and the Piql I/O (production) computer to connect the two. Only then can the malware alter the checksum on both computers' CPUs, which is necessary if state X wants to alter the client data undetected. Otherwise, the CPU on the Piql I/O computer would have picked up on the alternations to the checksum from the Piql computer's CPU during verification. This is why this type of sabotage is so demanding: one needs to alter the checksum on both CPUs or the alterations would not be successful. Unless the data owner has backup copies of what they sent to the Piql partner, these pieces of information are lost.	
Cause	
Type of risk (Hazard/Threat)	Threat: Logical sabotage of the information while stored electronically in the Piql IT system.

Intentional (Yes/No/Both)	Yes.
Profile of actor (if intentional)	State X wants to alter the details of diplomatic agreements to their advantage. One of the few countries in the world that is both capable of and willing to violate the privacy of other states for their own betterment. Though nothing can be definitively proven, state X has been involved in these kinds of operations before.
Description of cause	In removing some of the proof of agreements between itself and another country's Foreign Ministry, state X stands a better chance at altering the agreements to its benefit.
Competence and resources (if intentional)	State X has formidable resources and skills with regards to accessing other computer systems without authorisation. Employs many skilful hackers, whom they provide with a big support system.
User/value	
User class	Public sensitive.
User type	The Foreign Ministry.
Value	Sensitive diplomatic correspondence. Contains the details on how important bilateral decisions and agreements were made, which were not always above board. If it falls into the wrong hands, it could greatly damage the reputation of the Foreign Ministry and could potentially alter their future relationships with other nations who might now view them differently.
Location	
Location description	Geographical zone: South (Southern Africa). The region has varied terrain, ranging from forest and grasslands to desert. The developmental level is medium and the political climate is fairly stable. The piqlVault is situated in an urban area, near the city centre. The scenario takes place in the present. The time period is 0-30/50 years, as the value is time-sensitive, i.e. the diplomatic repercussions of such intelligence getting out is lessened with time. The scenario is also a risk for the future, or as long as diplomatic services have communications with other nations that they would like to hide.
Environment description	The climate zone is a warm temperate. It is winter, in early June. The local weather conditions are mild and hot and dry: 15° Celsius with a relative humidity of 57 %. The incident occurs at the start of the working day.

Production site description	The scenario takes place during the production of the piqlFilm. The setting is therefore the production site, which is situated in a standard office building. The Piql computer, the piqlWriter and the piqlReader are all located in the same large production room, whereas the processing room and its equipment are located elsewhere. The productions site is regulated through ventilation to uphold the ISO standards governing levels of humidity and temperature.
Local safety measures	We assume that all safety measures required by Piql AS to be in place in the storage facility also apply in the production site. See section 5.5.1 for details.
Local security measures	All security measures required by Piql AS are in place.
Consequences	
Outer building	The physical infrastructure of the building and the storage room is not affected during the incident.
Production site	The structural integrity of the production site is not affected by the incident. However, the Piql IT system, as part of the Piql Preservation Services, is breached. State X hackers are able, with the full weight and resources of state X behind them, to breach the security software of the Front-End code and gain access into the Piql computer system. Once there, the hackers place malware which utilises the interconnection between the Piql computer and the Piql I/O computer to completely connect the two. As the hackers now have free access to both computers' CPU they can alter the client data undetected because they also change the corresponding checksum on both CPUs. Even though the Piql I/O computer does what it is supposed to and checks the integrity of the data against the designated checksum, it can find no faults and confirms the data ready for writing on the piqlFilm.
Box	The piqlBox is not affected during the incident.
Film	The client information which is being prepared for writing onto the piqlFilm is accessed without authorised permission to the detriment of the data owner. It is altered to exclude certain important pieces of information. The complete information is thus prevented from being printed.
Power/energy supply	The power supply is not affected during the incident.
Divergence from ISO standard	The storage conditions of the Piql Preservation Services are not affected during the incident.

Security mechanisms	
Integrity	The integrity of the piqlFilm that is being printed was never intact to begin with, as the complete file of original information was never printed onto the film in its entirety. The integrity of the logical information stored in the Piql IT system was compromised when the alterations due to sabotage took place.
Availability	The availability of the information is forever lost, unless the data owner has backup copies.
Confidentiality	The confidentiality of the information was also breached the moment state X broke through the security software of the Front-End code and was able to access the client information to see which parts it wanted to alter.
Immunity (against attacks on the above mentioned)	The Piql Preservation Services is not immune to attacks against confidentiality, integrity and availability.
Recommendations	
Recommended protective measures	The IT security measures already in place are sound. Only a highly resourceful threat actor would be able to perform the sabotage outlined here. An option is to create a true air gap between the two computers' CPUs. Although this will not stop the threat actor from gaining access into the Piql IT system, it will make it impossible to alter the received client data undetected. However, such a measure is an unlikely feature in a production process, as it would make the production too inefficient.
References	
Relevant literature	

B.9 Espionage

Scenario number 9

Espionage

Scenario justification

Justification: When the value that is to be protected is information, the risk of espionage must be taken into account. Espionage involves tasks which can be undertaken by individuals, companies and, of course, states. Though espionage and intelligence gathering comes in many forms, of particular interest here is signals intelligence, or information gathered from the interception of signals. Depending on the sensitivity of the information stored on the piqlFilm, this kind of espionage must be planned for and protected against.

Purpose: As the Piql Preservation Services is an offline medium for the most part, any other form of espionage would somehow involve stealing the piqlFilm and reading its contents that way. Physical theft of this kind has been covered in other scenarios. This scenario we would rather use to demonstrate how the Piql Preservation Services can be subjected to logical theft, i.e. gaining unauthorised access to the signals carrying the information while it is electronically transferred inside a system. For the Piql Preservation Services, this is only possible during the production phase.

Benefit: This scenario seeks to illustrate how the Piql Preservation Services is vulnerable to threats against their IT system during the ingestion of the client data. Though the information stored using the Piql Preservation Services is offline for most of its existence, it is also online for a small period of time, and securing the information during this time is vital. The risks faced are the same for all services connected to a public web server, but that cannot minimise the importance of the Piql Preservation Services doing what it can to mitigate those risks.

Caveat: The Piql IT system is assessed to be well-secured, which means that it would take a threat actor with formidable abilities to break into the system logically. Therefore, this scenario presupposes that a state actor must be the culprit. A state actor would most likely spy on another state actor, often on some form of military intelligence or intelligence which could harm national security if it got out. We have to assume that if the Piql Preservation Services are used by a country’s Defence programme, then additional IT security would be put to meet that user’s very high security demands. However, for the sake of this assessment, we must analyse the possible risks based on the security regime set up by Piql AS. This scenario will illustrate the potential dangers of espionage to the other users who implement the IT security measures Piql stipulate, but be advised that the user in this scenario is unlikely to be as vulnerable. We must include the user, nonetheless, to gain a balance in the assessment.

Scenario outline

The scenario is set in the geographical zone North (North America). A threat actor with formidable skills in gaining unauthorised access into another’s IT system manages to break through the security software installed as part of the Piql IT system’s Front-End service. The state X, as we will call them, manages to install spyware on the Piql computer system which the security

measures in place are unable to detect. As a result, state X gains access to the designs of a weapon system developed by state Y, the major military power in the world. Though the designs are no longer state of the art by their standards, as state Y is so much further along all other states when it comes to military technology, the designs are a major breakthrough for state X to get their hands on. The malware copies these designs and sends them undetected to state X. State Y thus loses a major military advantage in possible future conflicts against state X.	
Cause	
Type of risk (Hazard/Threat)	Threat: Spyware installed on Piql computer system which duplicates the original file containing detailed descriptions of a new weapon system as it is prepared for printing.
Intentional (Yes/No/Both)	Yes.
Profile of actor (if intentional)	State X is regarded as one of the world's leading military powers, but it is still nowhere near the capacity of state Y, which has had the military upper hand for centuries now. Nevertheless, state X has formidable resources of its own and a perseverance which is unparalleled on the world stage when it comes to elevating their position. There are few things state X will not do to achieve this goal.
Description of cause	Espionage in the form of spyware installed on Piql receiving and processing computer which sends the prepared files to the piqlWriter. State X has viewed the latest political developments with regards to its relations with state Y with much alarm. The relations have worsened considerably the past few months, and state X fears a military strike by state Y is imminent. State X thus uses espionage to gain further knowledge of state Y's military capability, both to know what they are up against and to replicate state Y's military equipment to be able to defend themselves.
Competence and resources (if intentional)	As one of the world's leading military powers, state X has the resources, with regards to both finances and intelligence capabilities within the online realm, to go through with this kind of cyber operation.
User/value	
User class	Public sensitive.
User type	Military, defence. Military world power, state Y.
Value	Military secrets regarding the designs of a weapon system. As the technology is unknown to all other state actors, the loss of this asset will cause a major reduction in state Y's power position.

Location	
Location description	Geographical zone: North (North America). The developmental level is high and the political climate is stable. The piqlVault is situated in an urban area, located centrally in the city. The scenario takes place in the future, 2244, as it presupposes an imagined situation in which there are sufficient tensions between two highly developed military nations to make armed conflict imminent. The time period is 0-30/50 years, as the value is time-sensitive, i.e. once the military technology is sufficiently outdated it will be of no interest to spy on. The scenario is also a risk for the present, so long as the Piql Preservation Services store information which others are willing to go to great lengths to gain access to.
Environment description	The climate zone is a warm temperate climate. It is spring, in the end of April. The local weather conditions are fairly mild and dry: 12° Celsius with a relative humidity of 69 %. The plant of the malware happens in the middle of the night without being detected.
Production site description	The scenario takes place during the production of the piqlFilm. The setting is therefore the production site, which is situated in a standard office building. The Piql computer, the piqlWriter and the piqlReader are all located in the same large production room, whereas the processing room and equipment is located elsewhere. The productions site is regulated through ventilation to uphold the ISO standards governing levels of humidity and temperature.
Local safety measures	All safety measures required by Piql AS are in place, see section 5.5.1 for details.
Local security measures	All security measures required by Piql AS are in place.
Consequences	
Outer building	The physical infrastructure of the building and the storage room is not affected during the incident.
Production site	The structural integrity of the production site is not affected by the incident. However, the Piql IT system, as part of the Piql Preservation Services, is breached. A state X employee and professional hacker is able, with the full weight and resources of state X behind him/her, to breach the security software of the Front-End code and gain access into the Piql computer system. Here, the client data of state Y is being prepared for transfer over to the computer connected to the piqlWriter,

	meaning that state X has access to both the original files and the prepared file. The hacker installs a spyware which monitors the system and, upon finding something of interest, duplicates that information and transfers it back to a designated database owned by state X. All this is done undetected.
Box	The piqlBox is not affected during the incident.
Film	The information which is being prepared for writing onto a piqlFilm is not damaged or altered in any way, but the information is accessed without authorised permission to the detriment of the data owner.
Power/energy supply	The power supply is not affected during the incident.
Divergence from ISO standard	The storage conditions of the Piql Preservation Services are not affected during the incident.
Security mechanisms	
Integrity	As the piqlFilms are not damaged or altered during the incident, the data is not lost. The integrity of the piqlFilms thus remains intact.
Availability	The availability of the piqlFilms is not compromised, as the information is simply copied and not removed or damaged so that the data owner no longer has access to it. The availability of the information thus remains intact.
Confidentiality	Most importantly for the data owner, the confidentiality of the information about to be written onto the PiqlFilms was irrevocably compromised, as another actor who absolutely should not have had access to its contents did gain access. The loss of confidentiality also resulted in a significant loss of military advantage for the data owner.
Immunity (against attacks on the above mentioned)	The Piql Preservation Services is not immune to attacks against confidentiality.
Recommendations	
Recommended protective measures	Measures to mitigate against the threat of cyber-attacks include making sure that the security software used by the Piql partners is always state of the art; always keeping the security software up to date so as to secure the Piql IT system from unauthorised intrusion. Piql AS should offer encryption methods as part of their own security architecture to the users which value confidentiality higher than availability (as encryption inevitably results in loss of self-contained).

References	
Relevant literature	[70] Nasjonal sikkerhetsmyndighet (2015) *S-02 Ti viktige tiltak mot dataangrep.*

B.10 Terrorism

Scenario number 10

Terrorism

Scenario justification

Justification: In later years, terrorist attacks have become something we all must contend with. It is also impossible to know how this trend will progress. For now, the terrorist attacks tend to target people more than objects, but this may change. Objects are also damaged during the course of the attack, even though it was not the main target or intent of the terrorist(s). This scenario serves as a reminder to assess ones surroundings, not just with regards to natural disasters or obvious high risk occupancies like close proximity to chemical plants, but also taking into consideration the activities of your neighbours and if their actions and level of risk tolerance somehow affects and runs counter of your accepted level.

Purpose: The purpose of the scenario is to highlight the vulnerabilities of the Piql Preservation Services when placed in a building which is the target of a terrorist attack where homemade (and thus very volatile) bombs are involved.

Benefit: The benefit of this scenario for the PreservIA project is to emphasise the importance of constant vigilance, always being ready for an accident or incident, and not become complacent. Even if a Piql partner deems the circumstances of the Piql Preservation Services to be relatively safe and secure, it does not mean than they should lessen their safety and security measures. If terrorist attacks have shown us one thing, it is that one can never be sure of when or where they will strike, nor the amount of damage they can cause. Whether the Piql Preservation Services is the direct target of an attack or not, it can still simply be collateral damage because it was situated in the wrong place and the wrong time.

Scenario outline

The scenario is set in the geographical zone North (Southern Europe). The piqlVault is located in the same building as a major NGO advocating multiculturalism. One day, without warning, a lone right-wing extremist places a car bomb in front of the building and offices of said NGO and remote detonates the bomb. The Piql Preservation Services is collateral damage. The bomb is powerful enough to cause severe damage to the structural integrity of the building, and though the building does not collapse, it is still regarded as a large scale attack. The Piql Preservation Services is placed on the opposite side of the building to where the bomb is placed, meaning that the damage to the piqlVault is not as severe as the rest of the bottom floor. However, the bomb is powerful enough to cause great damage to the piqlVault. The pressure wave is powerful enough to knock the piqlVault system gird out of place, but the position of the grid near a wall and the tightly stacked Bins mean that the gird is simply tilted, rather than completely overturned.

Cause	
Type of risk (Hazard/Threat)	Threat: A bomb targeted at the office building where the piqlVault is located.
Intentional (Yes/No/Both)	Both. The threat to blow up the office building is intentional, but the direct target is not the piqlVault.
Profile of actor (if intentional)	A so-called lone wolf terrorist, with extreme right-wing sympathies. He/she does not have much of a social life, spends his/her days instead online in right-wing extremist chat rooms and the like. He/she has never done anything like this before, but has become more and more radicalised of late.
Description of cause	The right-wing extremist believes in white power and keeping societies homogenous. After allowing his/her rage against multiculturalism to build up unchecked for a long time, he/she decides to act. Online research leads him/her to the NGO in the same building as the piqlVault. Through recipes and description found on the internet, he/she builds a 500 kg bomb consisting of ammonium nitrate fertiliser. It causes all the windows in the building to blow out, the contents of the lower floors are almost entirely blown out by the pressure wave and an entire section of the building closest to the bomb is blown away.
Competence and resources (if intentional)	With endless supply of time and determination, the right-wing extremist manages to build the bomb he/she wants. He/she has some of the necessary skills from a lasting interest in chemistry, and gets tips online on how to acquire the relevant ingredients without being detected.
User/value	
User class	Business or private, sensitive information or not: the vulnerability is the same for all when the piqlVault is positioned in the damage radius of the bomb.
User type	Not relevant. See over.
Value	Not relevant. See over.
Location	
Location description	Geographical zone: North (Southern Europe). The continent’s landscape is marked by mountainous areas and flat, wide expanses and river valleys with mush vegetation. The developmental level of the continent is high and the political climate is stable. The piqlVault is situated in an urban area, right in the city centre. The scenario is set in 2029, and it could take place in the present and in

	the future. As the user class is undefined in this scenario, so is the time period, but it could apply for both: the result would be the same.
Environment description	The climate zone is temperate. It is winter, in the beginning of February. The local weather conditions are fairly cold and dry: 10° Celsius with a relative humidity of 70 % during the day and 4° Celsius and 45 % relative humidity during the night. The attack occurs mid-morning, to ensure that a maximum amount of people are at work.
Vault description	The scenario takes place while the piqlFilms are in storage in the piqlVault. The piqlVault system is placed in a storage room located in lower floors of an office building. The targeted organisation has offices on the same floor, but on the other side of the building. The vault is regulated through ventilation to uphold the ISO standards governing levels of humidity and temperature.
Local safety measures	All safety measures required by Piql AS are in place, see section 5.5.1 for details.
Local security measures	All security measures required by Piql AS are in place.
Consequences	
Outer building	The physical infrastructure of the building housing the NGO and the piqlVault suffers severe structural damage, but remains standing. Neither does the bomb cause a large fire, only smaller ones spread out. The power supply, however, is cut off due to damages to the electrical system. The structural integrity of the building is compromised to such an extent that it is unsafe to enter the building for several days before structural engineers have secured it and cleared it for entry.
Vault	The infrastructure of the storage room is also affected by the blast. The walls nearest to the position of the bomb are blasted apart, only arming is left. The contents of the piqlVault are exposed to the elements, as the walls surrounding the piqlVault or indeed the outer walls of the building are no longer whole. Additional loss of power makes maintaining the ideal storage conditions impossible. When the bomb blasts the walls of the storage room apart, some of the pieces of concrete hit the piqlVault system grid. The pressure wave causes the grid to shift out of its original position and tilt, but as it gets support from a back wall, it does not fall over. The tightly stacked piqlBins also help to stabilise the grid.
Box	The piqlBoxes slam into the side of the piqlBins with a significant amount of force when the pressure wave hits, but they do not open, and are otherwise not harmed. Even if they did open, the piqlFilm would not

	fall out, as the piqlBoxes are placed four to a piqlBin and stacked fairly tightly. However, some of the piqlBoxes are damaged by the pieces of concrete which are propelled into the grid. All of the piqlBoxes need to be replaced, however, as their structural integrity has been compromised and their longevity can no longer be guaranteed.
Film	The piqlFilms are not harmed by the explosive blast other than the pressure wave causing the piqlBoxes to slam into the piqlBins and thus shifting the piqlFilms a little inside the piqlBoxes. However, some of the piqlFilms are damaged by the pieces of concrete which are propelled into the grid. Even though the majority of the piqlFilms survived the initial blast and pressure wave, they are left exposed to the elements for several days before the building is declared safe for entry and the repair work can start. As it is winter in southern Europe when this scenario takes place, the effects on the piqlFilms are not very severe, as colder temperature and lower levels of humidity has less damaging effect on the piqlFilms than hotter temperatures and levels of humidity. The piqlFilms can become brittle and crispy when exposed to colder temperatures for longer periods of time, but so long as they are heated under controlled conditions before handling they should be fine.
Power/energy supply	The blast causes damage to electrical wiring, which means that the power supply is cut off and the ventilation shuts off. The backup generators are affected by this as well, so they cannot be put to use.
Divergence from ISO standard	The power supply to the piqlVault is completely cut off by explosive blast. Neither is the backup generator able to bring the power supply back up. The loss of ideal storage conditions is worsened when cold air is allowed to flow freely into the piqlVault, as the outer walls of the building and the storage room are gone.
Security mechanisms	
Integrity	The integrity of most of the piqlFilms remains intact during the explosion, as only the pressure wave and not the explosives themselves reach the piqlVault. The piqlFilms that are crushed by the pieces of concrete from the storage room wall are beyond repair and the integrity is forever lost. If the remaining piqlFilms are exposed to the cold temperature for too long, and they are not conditioned right before handling, this too may affect the integrity of the piqlFilms.
Availability	The availability of all the piqlFilms is compromised temporarily for two reasons: first, that the building was unsafe to enter for several days; and second, once Piql personnel could get into the building, due to the necessary repairs and, in part, demolition of the piqlVault system grid. As the grid was so badly tilted, the manual recovery mechanism was unavailable as well.

	For the piqlFilms which are damaged beyond repair by the flying concrete, availability is irrevocably compromised. For the piqlFilms which survive the colder temperatures, availability is only temporarily compromised while the Films are conditioned and prepared for safe handling again.
Confidentiality	The confidentiality of all the piqlFilms remains intact. All the piqlFilms in the vault were, however, left without proper security regarding access control when the outer walls protecting the piqlVault were blasted away and could hypothetically have been accessed by others at this time. Other circumstances (protected by the unstable infrastructure of the building) made sure no unwelcome persons came near the piqlFilms.
Immunity (against attacks on the above mentioned)	The Piql Preservation Services is not immune to attacks against integrity or availability.
Recommendations	
Recommended protective measures	As the risk in this scenario does not represent a direct targeting of the Piql Preservation Services, and it was rather collateral damage in another attack, the only advice one can give is “Beware of your surroundings”. All Piql partners must assess their surroundings and make a judgement call on the security level needed. Neither should they get complacent. When it comes to the specific mitigation against explosives, the recommendation from Piql AS to use an oxygen reduction suppression solution as the fire protection mechanism in the piqlVault is regarded as the best one. In this scenario, the fire did not reach the piqlVault, but when explosives are involved, it very well could have.
References	
Relevant literature	

B.11 Armed Conflict

Scenario number 11
Armed conflict with strategic assault
Scenario justification
Justification: A scenario regarding Svalbard/the Northern areas is highly relevant, as it illustrates how the world is not politically stable. We cannot be sure the placement of the piqlVault is a safe one for 500 years, as much can change in the world in that time. Just imagine the world map in the year 1500 compared to what it is today. The piqlVault can, in other words, not expect to be completely safe from armed conflict during its existence. Depending on the level of sensitivity of the information stored on the piqlFilms, the Piql Preservation Services may also be the target for a military operation which is part of a larger context. *Purpose*: The purpose of this scenario is to illustrate the most extreme kind of attack a piqlVault would need to withstand, if the information stored is sensitive enough. The security parameters in such a scenario are of course largely supplied by the data owner, but the Piql system would still be expected to provide certain protections. *Caveat*: The only scenario in which an armed attack on the Piql Preservation Services is plausible is if the piqlFilms store information which is a matter of national security. The only plausible storage facility for such information is within a mountain repository. Hence, this scenario must take place in a mountain hall, even though it has been previously stated that in all scenarios the piqlVault is placed in an industrial or office building. Due to the placement in a mountain hall, we must also assume that additional safety and security measures are in place.
Scenario outline
The scenario is set in the geographical zone North (Northern Areas, the Arctic). In a future setting a state actor X has set world domination as its foreign policy priority. Europe is the first region to be conquered. However, in order to launch a successful attack on the rest of Europe, state X needs to take from the enemy what it believes to be intelligence about state X' military capacity. This information could help the enemies of state X mount an effective defence against its future campaign in Europe when the time comes, and this must be prevented. After extensive planning, the state actor executes a night raid against the piqlVault, using EMWs and explosives to gain access to the facility. The EMW puts all electronic barriers around the perimeter out of commission, even manipulating the signals to allow access. Where that is insufficient, explosives and firepower is used to (controllably) blow open doors and put security guards out of action. State X successfully gains access to the storage room, which is not affected by the electromagnetic pulses, as it is placed inside the mountain hall. Had it been affected, the piqlVault system would not be functional. At gunpoint a Piql operator is commanded to order the pickup of the relevant piqlFilms, as well as several others to confuse the enemies of state X about its intent. Due to the remote location, the enemies of state X and the owner of the piqlFilms have been unable to summon backup in time, and state X leaves the way they came and disappear into the night.

Cause	
Type of risk (Hazard/Threat)	Threat: A strategic assault targeting the piqlVault as a build-up to a greater armed conflict.
Intentional (Yes/No/Both)	Yes.
Profile of actor (if intentional)	State X with a mind to take over the world. It is one of the most powerful states in a multipolar world system with a history of very erratic behaviour on the world stage. Has acted aggressively before, but has been left to its own devices as the other states do not want to provoke a full scale attack.
Description of cause	The state actor suspects the piqlVault in question is hiding intelligence about its military capacity. Believes it must gain a hold of these to launch a successful armed attack against the rest of Europe.
Competence and resources (if intentional)	The state actor has one of the world's largest stocks of very advanced military resources, both at sea, on land and in the air (which also includes EMWs).
User/value	
User class	Public sensitive.
User type	Military. Defence.
Value	Military intelligence regarding state X, which is seeking world domination. Without this information it will be more difficult to launch counterattacks against the future campaign of state X.
Location	
Location description	Geographical zone: North (Northern Areas, the Arctic). It is a mostly barren land, with snow-covered tundra and dangerous treks, which requires local knowledge to get about. Despite the harsh conditions, the developmental level is high and the political climate is stable, though the jurisdiction over the region is contested. The piqlVault is located in a remote location, far away from civilisation, as it is placed in a mountain hall. The scenario takes place in the future, 2346, as it presupposes an imagined situation in which a country seeks world dominance. The time period is 0-30/50 years, as the value is time-sensitive, i.e. the intelligence is only valid for so long due to state X's continuous military development. The scenario is also a risk for the present, so long as the Piql Preservation Services store information which others are willing to

	go to great lengths to gain access to.
Environment description	The climate zone is an arctic climate. It is winter, in the beginning of January. The local weather conditions are cold and dry: -23° Celsius with a relative humidity of 62 %. The attack is mounted at night. It is during the period of the polar night, but the timing is not due to the cover of darkness, but rather fewer people present in the piqlVault.
Vault description	The scenario takes place while the piqlFilm is in storage in the piqlVault. The piqlVault system is located in a mountain repository, deep in the permafrost. The vault is regulated through ventilation to uphold the ISO standards governing levels of humidity and temperature.
Local safety measures	All safety measures required by Piql AS are in place, see section 5.5.1 for details. Additional safety measures are in place, as befitting a mountain repository: Multiple backup generators, fortified walls with additional protection against nuclear blast, radiation, electromagnetic pulses and CBR agents.
Local security measures	All security measures required by Piql AS are in place. Additional security measures are in place, as befitting a high-demanding user: Access control: Protective barriers in the form of (i) gate monitored by security personnel for admittance, and (ii) doors/sluices inside the facility which opens with authorised ID verification solutions. Alarm systems: Alarm systems (i) installed in connection with authorisation devices, and (ii) triggered by motion sensors at strategic points. Summons security personnel. Camera surveillance: CCTV coverage of outside entrance area, all access points and all critical points inside the facility. Recorded and monitored 24/7. Security personnel: Two (2) guards onsite during office hours, one (1) onsite outside office hours. Sound vetting procedures for all personnel (either security clearance or criminal record and credit check depending on sector).
Consequences	
Outer building	The perimeter barriers around the entrance of the mountain hall are breached. They did not stand a chance against the direct military attack by state actor with formidable military powers. The use of EMWs cause all electronic barriers to fail, some even manipulated the signals in the system to allow access, and controlled explosions are used to force entry through doors which cannot be opened otherwise. This opens the facility

	up to the outside elements, but they do not reach the storage room, which is situated down a long corridor and separated by a door.
Vault	The piqlVault is forced entry, but strategically so, so that the structural integrity for the most part remains intact. The temperature and humidity regulations remain intact. The small fires caused by the controlled explosions needed to get into the storage room do not reach the piqlVault system grid (which would have been protected by the fire suppression mechanism anyhow). The weaponised electromagnetic pulses do not reach the piqlVault, as they were employed outside the mountain hall. Had they reached the piqlVault system, all operations would cease. The robots in particular could be damaged if there is an overload on several of its finer electronic components at the same time. The electromagnetic pulses would also destroy the data which is transferred via the radio signals from the Controller to the robots, impeding the movements of the robots.
Box	The piqlBox is not affected during the incident.
Film	The piqlFilms in question are not damaged. The electromagnetic pulses have no effect in the plastic of the film; the explosives and subsequent fire do not reach the vault; and the temperatures and humidity levels do not notably change. The piqlFilms are, however, removed from the facility without authorised permission.
Power/energy supply	The power supply is not affected in a notable way during the attack. The explosions were controlled to the extent that they would not take out any other systems while the doors were forced open. And even if they did, the mountain repository is well equipped with backup generators (no provider of redundancy, however, as too difficult due to remote location).
Divergence from ISO standard	The storage conditions of the Piql Preservation Services are not notably affected during the incident. The entrance to the storage room is left open after the state actor leaves, as the door has been blown away, but the backup that was called by the data owner during the attack arrive fairly quickly after state X left and were able to restore ideal storage conditions.
Security mechanisms	
Integrity	As the piqlFilms are not damaged during the incident, the data is not lost in the sense that it is altered. The integrity of the piqlFilms thus remains intact.
Availability	The availability of the piqlFilms is compromised, as the information stored on them is no longer accessible to the data owner.

Confidentiality	Most importantly for the data owner, the confidentiality of the information stored on the PiqlFilms was irrevocably compromised, as another actor who absolutely should not have had access to its contents did gain access. The loss of confidentiality may have grave consequences for the data owner, insofar as they are unable to defend themselves during the imminent attack as well as they potentially would have been.
Immunity (against attacks on the above mentioned)	The Piql Preservation Services is not immune to attacks against confidentiality and availability.
Recommendations	
Recommended protective measures	Taking necessary precautions and constantly being alert and aware of potential risks. Ensuring the data is backed-up regularly during a period marked by geopolitical tensions, in case of an imminent attack.
References	
Relevant literature	[85] Landbruks- og matdepartementet (n.d.), *Svalbard Globale frøhvelv* [56] Heireng, H. S., Elgsaas, I. M., Nystuen, K. O., et.al (2014), "*Nasjonale verdier står på spill – hva koster mangelfull forebyggende sikkerhet det norske samfunn?"* [86] Ekspertgruppen for Forsvaret av Norge (2015), *Et felles løft*

B.12 Nuclear War

<table>
<tr><th colspan="2">Scenario number 12</th></tr>
<tr><td colspan="2"><b>Nuclear war</b></td></tr>
<tr><td colspan="2"><b>Scenario justification</b></td></tr>
<tr><td colspan="2"><i>Justification</i>: The event of a nuclear bomb is included in the assessment as one representation of all the improbable events that may affect the Piql Preservation Services during the course of 500 years. Yet, we cannot categorically rule out that they will occur as the level of uncertainty is so high in this assessment, so they must be included. We chose this as our unlikely scenario, as the effects of nuclear detonations have been demonstrated, and as such we can apply these to the Piql Preservation Services, as opposed to an event we have no knowledge of.
<i>Purpose</i>: The purpose of the scenario is also connected to the level of uncertainty associated with the longevity of 500 years. Its main goal is to emphasise the fact that during the course of such a long time the Piql Preservation Services can be caught in something that is much bigger than itself, making its safety and security depend on events and decisions far outside its control. In such a situation, being able to correctly analyse ones situation and ones surroundings, and most importantly be willing to quickly adapt to new situations is vital. In this case, such willingness can allow the Piql Preservation Services to be moved out of harm’s way, or be annihilated along with everything else when the nuclear detonation is a fact.</td></tr>
<tr><td colspan="2"><b>Scenario outline</b></td></tr>
<tr><td colspan="2">The scenario is set in the geographical zone Middle (Middle East). In a future setting, the days of Mutually Assured Destruction (MAD) are back, yet the situation is different than it was during the 20th century. There are a greater number of active nuclear powers now, all of whom use deterrence as their main policy. This means that the proliferation of nuclear weapons is higher than ever before and more regions of the world are directly exposed to the threat. Countless warheads are directed at various major cities at all times. One such city is a major metropolis in the Middle East. A glitch in the launch system of a major nuclear power releases a missile on said city by mistake. Even though the piqlVault is not situated within the radius of ground zero where heavily built concrete structures are severely damaged and fatalities approach 100 %, it is still within the air blast and thermal radiation radius where most residential houses collapse and fatalities are widespread. The Piql Preservation Services is not the main target – it was simply placed in an area more vulnerable to an attack – and because of that it is destroyed as a casualty of war.</td></tr>
<tr><td colspan="2"><b>Cause</b></td></tr>
<tr><td>Type of risk (Hazard/Threat)</td><td>Threat: A thermal nuclear detonation. The global political environment is such that you have a nuclear warhead directed at your city at all times.</td></tr>
<tr><td>Intentional (Yes/No/Both)</td><td>Both. The threat is intentional, i.e. to have a nuclear warhead directed at the city at all time, but the actual detonation was an accident caused by a malfunctioning launch system.</td></tr>
</table>

Profile of actor (if intentional)	Major nuclear power with nuclear warheads directed at various targets at all times.
Description of cause	Due to the global political environment and the policy of MAD, the Middle Eastern city is targeted with a nuclear warhead. However, its detonation was an accident. The threat actor had no real intention of launching the missile. The nuclear warhead detonated weighs 300 kiloton, which, when detonated in the air above the target, as good as annihilates everything in a 7.5 km radius from ground zero. The destruction is caused either by the initial fireball or blast wave or the mass fire ignited as a consequence of the former. The area most affect by the radioactive fallout depends on the wind direction and where the smoke and mushroom cloud are carried.
Competence and resources (if intentional)	The threat actor is one of several acknowledged nuclear powers. They have done nuclear weapons testing, which has been verified by other nations as being successful.
User/value	
User class	Business or private, sensitive information or not: the vulnerability is the same for all when the piqlVault is positioned in the damage radius of the nuclear detonation.
User type	Not relevant. See over.
Value	Not relevant. See over.
Location	
Location description	Geographical zone: Middle (Middle East). The setting is a major Middle Eastern metropolis. The developmental level is not very high, and construction techniques are not very modern or advanced. The piqlVault is situated in an urban area, centrally located in the city. The scenario takes place in the future, 2399, as it presupposes an imagined situation in which the days of MAD are back. As the user class is undefined in this scenario, so is the time period, but it could apply for both: the result would be the same.
Environment description	The climate zone is hot desert with very little precipitation. It is autumn, the beginning of October. The local weather conditions are mild and dry: 18° Celsius with a relative humidity of 41 %. The incident occurs late afternoon.
Vault description	The scenario takes place while the piqlFilms are in storage in the piqlVault. The piqlVault system is placed in a storage room located in the

	lower floors of an office building. The vault is regulated through ventilation to uphold the ISO standards governing levels of humidity and temperature.
Local safety measures	All safety measures required by Piql AS are in place, see section 5.5.1 for details.
Local security measures	All security measures required by Piql AS are in place.
Consequences	
Outer building	The physical infrastructure of the building housing the piqlVault suffers severe structural damage from the initial blast wave. The building is caught in the mass fire shortly after, which rages for hours at extreme temperatures. The building, and everything in it, is no more.
Vault	The infrastructure of the storage room and the piqlVault system suffers the same fate as the building within which it is place.
Box	The piqlBoxes all melt during the mass fire.
Film	The piqlFilms all melt during the mass fire. However, image a slightly different scenario: Were the piqlFilms located outside of the thermal radiation radius, i.e. just out of reach of the destruction caused by the detonation but instead exposed to the maximum amount of radiation from the radioactive fallout, the piqlFilms would suffer exposure to high-energy radiation over a long period of time. Because of the mass fire and the consequent intense heat and the danger to exposure, no personnel can get near the piqlFilms for days. The high levels of radiation will do little to the integrity of the information on the piqlFilms, but it will result in reduced longevity for the physical medium.
Power/energy supply	As the building which houses the piqlVault is destroyed, this is not relevant.
Divergence from ISO standard	As the building which houses the piqlVault is destroyed, this is not relevant.
Security mechanisms	
Integrity	The integrity of all the piqlFilms is compromised, as none of them retained their physical structure after the detonation and the data is lost.
Availability	The availability of all the piqlFilms is compromised, as they all were completely destroyed after the detonation and as such never accessible again.

Confidentiality	The confidentiality of all the piqlFilms remains intact during the incident, as no one could access the piqlVault while it was still standing. After it was destroyed, the information on the piqlFilms was no longer accessible to the data owner, but neither was it accessible to anybody else.
Immunity (against attacks on the above mentioned)	The Piql Preservation Services is not immune to attacks against integrity or availability.
Recommendations	
Recommended protective measures	The consequences of a doomsday scenario such as this are difficult to mitigate against. The only option is to be realistic and foresighted enough to move the piqlVault out of harm's way. In this scenario, that would mean out of any major city, and even there one can never be entirely safe from the radioactive fallout. The best protection one can give the piqlVault from a nuclear strike, is placing it in a mountain hall. Yet, even there it might not be safe from a direct hit given the strength of today's weapons, and probably also the future's.
References	
Relevant literature	[50] Glasstone S., Dolan P. J. (eds.) (1977) *The Effects of Nuclear Weapons* [87] Wellerstein, A. (2014) *Nukemap* [88] Starr, S. (2005), *The Effects of a 300 kiloton Nuclear Warhead Detonated Above Washington, D.C.*

Appendix C Storage Room Calculations

C.1 Temperature Increase in Storage Room

Calculations by Odd Busmundrud, FFI

Temperature change in a system can be calculated from the energy flow and heat capacity. dT/dt=(energy input minus energy loss)/(heat capacity), where dT/dt is temperature change per time.

In the case of the storage room, the energy input is the electrical power supplied to the room. (Supposing there is no other energy source, like external heating)

The energy loss is thermal energy transported out of the room by air flow, and by conduction through walls, ceiling and floor.

Energy input

Each robot has an average power consumption of 78 W.

The charger has a power consumption of 1840 W during charging. The charging of two 12 V 105 Ah batteries would take approximately 3 hours, supposing 50% efficiency.

The total average power consumption of one robot (including charging) can be calculated to be approximately 150 W.

In addition there are probably other energy sources like lightning and data equipment. There is not sufficient information on this. However, suppose there are ten 60W light bulbs in the room, this would add another 600 W.

Also, if there is one data server and other data equipment, an educated guess is that this could add another 500W.

The total energy input to the room, with two robots, would then be approximately 1400.

With no lightning, this would be reduced to 800 W.

With all data equipment outside the room, the power input would be further reduced to 300 W.

The total energy input could then be estimated to be between 300 and 1400 W.

Heat capacity

The heat capacity of the room consists of the heat capacity of the air in the room, and the heat capacity of equipment in the room and the room walls.

The volume of the room is 640 m^3. At a temperature of 20° Celsius, the air mass would be 760 kg. The specific heat capacity of air at constant pressure is very close to 1kJ/kg/K (1K = 1 degree C), so the total heat capacity of the air in the room is 760 kJ/K.

There is no specific information on other equipment. However, the stored items seem to be composed of polymer bins, possibly on aluminium shelves. Supposing that the total mass load on the floor is 1000 kg/m^2, and half the room is filled up with this, the total mass inside the room would be 43000 kg. The heat capacity of aluminium is 0,9 kJ/kg/K, and polyethylene is 1,5 kJ/ kg/K. This would make the total heat capacity of the equipment inside to 52000 kJ/K (supposing half and half aluminium and polyethylene). In addition, the walls have a heat capacity, but given the large uncertainties, this is not taken into account.

Calculation of temperature rise

Given the lack of information of the items in the room, the temperature rise of the empty room is first calculated, with only the robots working inside, and no energy loss to the outside.

Empty room

Heat capacity 760 kJ/K

Energy input 1400 W: dT/t=1400/760000 = 0,0018 K/s = 6,6 K/hour

Energy input 300 W: dT/t=300/760000 = 0,0004 K/s = 1,4 K/hour

Room with 43 tons equipment

Heat capacity 52760 kJ/K

Energy input 1400 W: dT/t=1400/52760000 = 0,000027 K/s = 0,096 K/hour

Energy input 300 W: dT/t=300/52760000 = 0,0000057 K/s = 0,02 K/hour

Energy loss

The above calculations do not take into account loss of energy from the room, but suppose that the room is thermally insulated from the surroundings. This is obviously not the case. Thermal energy will be exchanged with the surroundings by conduction through walls, ceiling and floor, and by exchange of air, even if the ventilation system is not working. Which way the energy travels depends on the temperature difference. One factor here is time of the year. Due to lack of information, this cannot be calculated.

Conclusions

Given the limited information available, the following figures can be calculated.

The temperature rise for an empty room, but with robots at work inside is between 1,4 and 6,6 K/hour (1 K=1 degree C). Obviously, the robots will not be working inside an empty room:

With inside equipment based on an educated guess, the temperature rise will be between 0,02 and 0,1 K/hour.

If more information could be made available, more accurate calculations could be performed.

References

[1] T. Cadell (1823), *A New Translation of Aristotle's Rhetoric* [E-book]. Available at: Google Books https://books.google.no/books?id=wy1jmQlIEPAC&printsec=frontcover&hl=no&source= gbs_ge_summary_r&cad=0#v=onepage&q&f=false [Accessed 01.04.16].

[2] Piql AS (2015), "*PreservIA EUREKA project application form".* Project number BIA 245586-Eureka.

[3] Piql AS (2014), "*Creating the Ultimate Digital Insurance: Behind the Curtains*".

[4] Piql AS (2014), "*What We Do Behind the Scenes*".

[5] Standard Norge (2009), "*Risikostyring. Terminologi. Risk Management Terminology*". Standard Norge SN-ISO Guide 73:2009. Standard Norge.

[6] Norsk Standard (NS) (2014), "*Samfunnssikkerhet. Beskyttelse mot tilsiktede uønskede handlinger. Krav til styringsrisikoanalyse*". Norsk standard NS 5832:2014. Standard Norge.

[7] Busmundrud, O., Maal, M., Kiran, J. H., et.al (2015), "*Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger*". FFI-rapport 2015/00923. Forsvarets forskningsinstitutt.

[8] Rausland, M., Utne, I. B. (2009), *Risikoanalyse – teori og metoder*. Trondheim: Tapir Akademisk Forlag.

[9] Element Logic (2015), "*AutoStore System Specification, Version 13.8*".

[10] Øverlier, L., Broen, T., Busmundrud, O., et.al (2013), "*IKT- og CBR-trusler mot Oslo vann og avløp*". [B] FFI-rapport 2013/03052. Forsvarets forskningsinstitutt.

[11] NOU (2000:24), "*Et sårbart samfunn. Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet*". Oslo: Departementenes servicesenter.

[12] NOU (2006:6), "*Når sikkerhet er viktigst. Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner*". Oslo: Departementenes servicesenter.

[13] Norsk Standard (NS) (2012), "*Samfunnssikkerhet. Beskyttelse mot tilsiktede uønskede handlinger. Terminologi*". Norsk standard NS 5830:2012. Standard Norge.

[14] Forskrift om informasjonssikkerhet (2001), Forskrift 1. juli 2001 nr. 744 om informasjonssikkerhet (Regulations for Information Security [freely translated]).

[15] Forsvarsdepartementet (2014), "*Forsvarsdepartementets retningslinjer for informasjonssikkerhet og cyberoperasjoner i forsvarssektoren*" (The Guidelines of the Ministry of Defence on Information Security and Cyber Operations in the Defence Sector [freely translated]) [Online]. Oslo: Forsvarsdepartementet. Available from: https://www.regjeringen.no/no/aktuelt/Nye-retningslinjer-for-informasjonssikkerhet-og-cyberoperasjoner-i-forsvarssektoren-/id753949/ [Accessed 02.09.15].

[16] Gollmann, D. (2011), *Computer Security*. West Sussex: John Wiley & Sons, Ltd.

[17] Riksarkivet (2010), "*Digitalt og autentisk – Planlegging av Arkivverkets nye depotløsning for digitalt skapt arkivmateriale, kortversjon*" [Elmag-2 rapporten]. Riksarkivet, Available from: http://docplayer.no/7347684-Digitalt-og-autentisk-planlegging-av-ny-depotlosning-for-arkivverkets-digitalt-skapte-arkivmateriale-prosjektrapport.html.[Accessed 27.05.15].

[18] Sikkerhetsloven (1998), Lov 20. mars 1998, nr. 10 om forebyggende sikkerhetstjeneste. (Act relating to Protective Security Services [freely translated]).

[19] Kottek, M., Grieser, J., Beck, C. et. al (2006) "*World Map of the Köppen-Geiger climate classification updated"*, in: *Meteorologische Zeitschrift*, Vol. 15(3), June, pp. 259-263(5).

[20] Peel, M. C., Finlayson, B. L., and McMahon, T. A. (2007), "*Updated world map of the Köppen-Geiger climate classification*", in: *Hydrology and Earth System Sciences* [e-journal], Vol.11(5), pp.1633-1644, DOI:10.5194/hess-11-1633-2007. Available from: http://data.worldbank.org/indicator [Accessed 03.06.15].

[21] World Bank (n.d.) *World Development Indicators*. [Online]. Available from: http://data.worldbank.org/indicator [Accessed 03.06.15].

[22] World Bank (n.d.) *World Governance Indicators*. [Online]. Available from: http://info.worldbank.org/governance/wgi/index.aspx#home [Accessed 03.06.15].

[23] Forskrift om offentlige arkiv (1998), Forskrift 11. desember 1998 nr. 1193 om utfyllende tekniske og arkivfaglige bestemmelser for offentlige arkiver (Regulations on Public Archives [freely translated]).

[24] Offentlighetsloven (2006), Lov 19. mai 2006 nr. 16 om rett til innsyn i dokument i offentleg verksnemd. (Act relating to public access to documents in the public administration [Freedom of Information Act] [freely translated]).

[25] Beskyttelsesinstruksen (1972), Instruks 17. mars 1972 nr. 3352 for behandling av dokumenter som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven med forskrifter. (Instructions on the management of information in need of protection for other reasons than those mentioned in the national act on protective security services, including regulations [freely translated]).

[26] Personopplysningsloven (2000), Lov 14. april 2000 nr. 31 om behandling av personopplysninger. (Act relating to the Processing of Personal Data [Personal Data Act]) [freely translated]).

[27] Piql AS (2016), "*Storage Conditions and Security Requirements: PiqlVault*". Technical Memo in PreservIA project (BIA 245586-Eureka).

[28] The International Organization for Standardization (ISO) (2010), "*Imaging Material – Processed Safety Photographic Films – Storage Practices*" [Online]. ISO 18911:2010. Available from: http://www.iso.org/iso/catalogue_detail.htm?csnumber=46602 [Accessed 01.06.15].

[29] Skjølberg, T. (2015), "*AutoStore Recovery Handling of Bin*". Technical Memo in AStoR project **(**Project Number 219744), WP AS4e. Element Logic AS.

[30] Nikolaisen, T. (ed.) (2005), *Sikringshåndboka. Håndbok i sikring og beskyttelse av eiendom, bygg og anlegg mot terrorhandlinger, spionasje, sabotasje og annen kriminalitet*. [Unntatt offentlighet]. 3. utg. Oslo: Idé Trykk AS.

[31] Content Delivery & Security Association (CDSA) (2016) "*Content Protection & Security Standard". *[Online]. Available from: http://www.cdsaonline.org/wp-content/uploads/2016/02/Content-Protection-Security-Standard-February-2016.pdf [Accessed 24.11.15.]

[32] Piql AS (2016), "*Pre-Installation Procedure*". Technical document for use during installation of the Piql system at Piql partner in Brazil.

[33] Piql AS (2012), "*Piql Preservation System Architecture and Security*". Technical Note in Archivator project (E! 4863).

[34] Piql AS (2012), "*Piql Preservation System Development Methodology*".

[35] Brudeli, B. H. (2012), "*Description of security applications regarding the client interface to the outside world*". Technical Note in Archivator project (E! 4863). Piql AS.

[36] Taleb N. N. (2010), *The Black Swan: The Impact of the Highly Improbable*. London: Penguin Books.

[37] Norheim-Martinsen, P. M. (2011), "*Trender, scenarioer og sorte svaner – utfordringer for fremtidens landmakt*". FFI-rapport 2011/01667. Forsvarets forskningsinstitutt.

[38] Øverland, E. F., Karlsen, J. E. (2010), *Carpe Futurum! Kunsten å forberede seg på fremtiden* Oslo: Cappelen Damm akademisk.

[39] Johansen, I. (2014), "*En morfologisk analyse av scenarioklasser for norske spesialstyrker – metode og tilnærming".* FFI-notat 2014/00438. Forsvarets forskningsinstitutt.

[40] Johansen, I. (2006), "*Scenarioklasser i Forsvarsstudie 2007: En morfologisk analyse av sikkerhetspolitiske utfordringer mot Norge"*. FFI-rapport 2006/02664. Forsvarets forskningsinstitutt.

[41] Zwicky, F. (1969), *Discovery, Invention, Research through the Morphological Approach.* Toronto: The Macmillan Company.

[42] Stenström, M. (2011), "*Morfologisk analys i grupp:En personlig handledning*". FOI-rapport FOI-R—3215—SE. Totalförsvarets Forskningsinstitut.

[43] Meyer, S. (2008), "*Typologi over uønskede hendelser".* FFI-rapport 2009/00447. Forsvarets forskningsinstitutt.

[44] Oxford (2006), *Concise Oxford English Dictionary.* Oxford: Oxford University Press

[45] Forsvarsdepartementet og Justis- og beredskapsdepartementet (2015), "*Støtte og samarbeid. En beskrivelse av totalforsvaret i dag"* [Online]. Oslo: Forsvarsdepartementet. Available from: https://www.regjeringen.no/no/aktuelt/ny-publikasjon-dette-er-totalforsvaret/id2473431/ [Accessed 28.04.15].

[46] Endregard, M., Breivik, H., Heireng, H. S., et.al (2011), "D2.1 Scenario Template, Existing CBRN Scenarios and Historical incidents". Published as a PRACTICE WP2 Deliverable. Forsvarets Forskningsinstitutt.

[47] The Engineering Toolbox (n.d.), *Metals - Melting temperatures* [Online]. Available from: http://www.engineeringtoolbox.com/melting-temperature-metals-d_860.html [Accessed 30.11.15].

[48] The Engineering Toolbox (n.d.), *Chemical Resistance of PolyPropylene* [Online]. Available from: http://www.engineeringtoolbox.com/polypropylene-pp-chemical-resistance-d_435.html [Accessed 20.11.15].

[49] The Engineering Toolbox (n.d.), *Chemical Resistance of Polyesters* [Online]. Available from: http://www.engineeringtoolbox.com/chemical-resistance-polyester-d_784.html [Accessed 20.11.15].

[50] Glasstone S., Dolan P. J. (eds.) (1977) *The Effects of Nuclear Weapons*. 3rd ed. United States Department of Defense and the United States Department of Energy.

[51] N. J. Broadway, S. Palinchak (1964), "*The Effect of Nuclear Radiation on Elastomeric and Plastic Components and Materials, Addendum*" [Online]. Defense Documentation Center for Scientific and Technical Information. Ohio: Battelle Memorial Columbus Ohio. Available from: http://www.dtic.mil/dtic/tr/fulltext/u2/454056.pdf [Accessed 01.12.15].

[52] Leszczynski, D. (2013), *Radiation Proteomics: The effects of ionizing and non-ionizing radiation on cells and tissues* [E-book]. Available at: Google Books https://books.google.no/books?id=ZcBEAAAAQBAJ&printsec=frontcover&hl=no&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false [Accessed 20.05.16].

[53] Shimizu, N., Hirata, K., Hasegawa, K., et.al (2007) "*Dose dependence of Radiation Damage for Protein Crystals Studied at Various X-Ray Energies*", in: *Journal of Synchrotron Radiation* [e-journal], 2007 Jan, Vol.14(Pt.1), pp.4-10. Epub 2006 Dec 15. Available from: http://www.ncbi.nlm.nih.gov/pubmed/17211067 [Accessed 20.05.16].

[54] Takeshita, K. (1975), "*Dose Estimation from Residual and Fallout Radioactivity*", in: *Journal of Radiation Research* [e-journal], Vol.16 (Suppl 1), pp-24-31, DOI:10.1269/jrr.16.Suppl_1.24. Available from: http://jrr.oxfordjournals.org/content/16/Suppl_1/24.full.pdf+html [Accessed 20.05.16].

[55] Grønhaug, K. L. (2003), "*Elektromagnetiske våpen*". I: Riis L., Holm K. B., and Ommedal J. (eds), *Håndbok i våpenvirkninger*. [Unntatt offentlighet]. Forsvarsbygg. Kap.7.

[56] Heireng, H. S., Elgsaas, I. M., Nystuen, K. O., et.al (2014), "*Nasjonale verdier står på spill – hva koster mangelfull forebyggende sikkerhet det norske samfunn?".* [B] FFI-rapport 2013/01189. Forsvarets forskningsinstitutt.

[57] Piql AS (2013), "*Alternative Storage Technologies*". Whitepaper.

[58] Merian, L. (2014), *WD leapfrogs Seagate with world's highest capacity10 TB helium drive, new flash drives* [Online]. Available from:

http://www.computerworld.com/article/2604311/computer-hardware/wd-leapfrogs-seagate-with-world-s-highest-capacity-10tb-helium-drive-new-flash-drives.html [Accessed 30.03.16.]

[59] Teach-ict (n.d) *Hard Disk* [Online]. Available fromhttp://www.teach-ict.com/as_a2_ict_new/ocr/AS_G061/312_software_hardware/storage_devices/miniweb/pg5.htm [Accessed 30.03.16].

[60] Beach, B. (2013), *How long do disk drives last?* [Online]. Available from: https://www.backblaze.com/blog/how-long-do-disk-drives-last/ [Accessed 30.03.16.]

[61] Zandbergen, P. (n.d.), *What Is an Optical Drive? –Definition, Types & Fuction* [Online]. Available from: http://study.com/academy/lesson/what-is-an-optical-drive-definition-types-function.html [Accessed 30.03.16.]

[62] Bradley, K. (2006), *Risks Associated with the Use of Recordable CDs and DVDs as Reliable Storage Media in Archival Collections – Strategies and Alternatives* [Online]. Memory of the World Programme, UNESCO. Available from: http://unesdoc.unesco.org/images/0014/001477/147782E.pdf [Accessed 30.03.16.]

[63] Computer Hope (n.d.), *Optical disc* [Online]. Available from: http://www.computerhope.com/jargon/o/optidisc.htm [Accessed 30.03.16.]

[64] Morgan, C. (n.d.), *Data storage lifespans: How long will media really last?* [Online]. Available from: http://www.storagecraft.com/blog/data-storage-lifespan/ [Accessed 30.03.16.]

[65] Mellor, Chris (2015), *LTO Issues Mighty Seventh-Generation 15TB Tape Format* [Online]. Available from: http://www.theregister.co.uk/2015/09/16/lto_has_15tb_gen_7_tape_format/ [Accessed 25.04.16.]

[66] Shinder, D. L. and Cross M. (2008), *Scene of the Cybercrime.* [E-book]. Available at: Google Books https://books.google.no/books?id=fJVcgl8IJs4C&printsec=frontcover&hl=no&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false [Accessed 01.04.16].

[67] Technicolor (2013). "*Securing Media Data Archives for Hundreds of Years*". Archiving Whitepaper.

[68] Hitachi Data Systems (2014). "*Reduce Cost and Risks for Data Migrations: Data Migration Best Practices and Nondisruptive Migration Service Capability for Enterprise Storage*". Whitepaper.

[69] WBDG Secure/Safe Committee (2015), *Natural Hazard Mitigation* [Online]. Available from: https://www.wbdg.org/design/resist_hazards.php [Accessed 30.03.16].

[70] Nasjonal sikkerhetsmyndighet (2015) *S-02 Ti viktige tiltak mot dataangrep.* Available from: https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/s-02-ti-viktige-tiltak-mot-dataangrep.pdf [Accessed 10.03.16.]

[71] Weaver, G. (2008), "*A Guide to Fiber-Base Gelatin Silver Print Condition and Deterioration*". George Eastman House, International Museum of Photography and Film. Available from: http://gawainweaver.com/images/uploads/Weaver_Guide_to_Gelatin_Silver.pdf [Accessed 20.05.16].

[72] Merriam-Webster (n.d.), *Merriam-Webster dictionary Online* [Online]. Available from: http://www.merriam-webster.com [Accessed 15.10.15].

[73] United Nations (1997), "*General and Complete Disarmament: Small Arms*" [Online]. A/52/298. Available from: http://www.unodc.org/documents/organized-crime/Firearms/ITI.pdf http://www.un.org/Depts/ddar/Firstcom/SGreport52/a52298.html [Accessed 08.12.15].

[74] National Institute for Occupational Safety and Health (NIOSH) Education and Information Division (2011), *Chlorine: Lung Damaging Agent* [Online]. Centers for Disease Control and Prevention. Available from: http://www.cdc.gov/niosh/ershdb/emergencyresponsecard_29750024.html [Accessed 29.11.15].

[75] CAMEO Chemicals (n.d.), *Chlorine* [Online]. Available from: http://cameochemicals.noaa.gov/chemical/2862 [Accessed 29.11.15].

[76] The Royal Society of Chemistry (n.d.), *Reactions of chlorine, bromine and iodine with aluminum* [Online]. Available from: http://www.rsc.org/learn-chemistry/resource/res00001766/reactions-of-chlorine-bromine-and-iodine-with-aluminium?cmpid=CMP00005276 [Accessed 29.11.15].

[77] Babrauskas, V. (1997), *Temperatures in flames and fires* [Online]. Fire Science and Technology Inc. Available from: http://www.doctorfire.com/flametmp.html [Accessed 01.12.15].

[78] Elval (n.d.), *Aluminium & Fire* [Online]. Available from: http://www.elval.gr/default.asp?pid=185&la=2 [Accessed 30.11.15.]

[79] Summers, P. T., Chen, Y., Rippe, C. M. et. al. (2015), *"Overview of aluminum alloy mechanical properties during and after fires"*, in*: Fire Science Reviews* [e-journal], Vol. 4(3). Available from: http://www.firesciencereviews.com/content/4/1/3 [Accessed 01.12.15].

[80] FloodList (n.d.), *Asia* [Online]. Available from: http://floodlist.com/ [Accessed 14.10.15].

[81] Gabbert, B. (2011), *At what temperature does a forest fire burn?* [Online]. Wildfire Today. Available from: http://wildfiretoday.com/2011/02/26/at-what-temperature-does-a-forest-fire-burn/ [Accessed 17.10.15].

[82] Kriseinfo.no (n.d.), *What is a forest fire?* [Online]. Available from: http://www.kriseinfo.no/en/Fire-and-explosions/Forest-fires/What-is-a-forest-fire/ [Accessed 17.10.15].

[83] Lundin Norway AS (n.d.), *Letestrategi* [Online]. Available from: http://lundin-norway.no/blog/2013/03/20/letestrategi/ [Accessed 04.11.15].

[84] Security Incorporated Corp. (n.d.), *Armored Transport Service* [Online]. Available from: http://www.securityincorporated.com/armored-transportation.htm [Accessed 04.11.15].

[85] Landbruks- og matdepartementet (n.d.), *Svalbard Globale frøhvelv* [Online]. Regjeringen.no. Available from: https://www.regjeringen.no/no/tema/mat-fiske-og-landbruk/landbruk/svalbard_global_frohvelv/id462220/ [Accessed 10.08.15].

[86] Ekspertgruppen for Forsvaret av Norge (2015), *Et felles løft* [Online]. Forsvarsdepartementet, Regjeringen.no. Available from: https://www.regjeringen.no/no/dokumenter/et-felles-loft---fra-ekspergruppen-for-forsvaret-av-norge/id2427726/ [Accessed 26.05.15].

[87] Wellerstein, A. (2014) *Nukemap* [Online]. Available from: http://nuclearsecrecy.com/nukemap/?&kt=300&lat=35.696111&lng=51.423056&hob_ft=0&zm=13 [Accessed 18.03.16].

[88] Starr, S. (2005), *The Effects of a 300 kiloton Nuclear Warhead Detonated Above Washington, D.C.* [Online]. The Nuclear Age Peace Foundation. Available from: https://www.wagingpeace.org/the-effects-of-a-300-kiloton-nuclear-warhead-detonated-above-washington-d-c/ [Accessed 18.03.16].

About FFI

The Norwegian Defence Research Establishment (FFI) was founded 11th of April 1946. It is organised as an administrative agency subordinate to the Ministry of Defence.

FFI's MISSION

FFI is the prime institution responsible for defence related research in Norway. Its principal mission is to carry out research and development to meet the requirements of the Armed Forces. FFI has the role of chief adviser to the political and military leadership. In particular, the institute shall focus on aspects of the development in science and technology that can influence our security policy or defence planning.

FFI's VISION

FFI turns knowledge and ideas into an efficient defence.

FFI's CHARACTERISTICS

Creative, daring, broad-minded and responsible.

Om FFI

Forsvarets forskningsinstitutt ble etablert 11. april 1946. Instituttet er organisert som et forvaltningsorgan med særskilte fullmakter underlagt Forsvarsdepartementet.

FFIs FORMÅL

Forsvarets forskningsinstitutt er Forsvarets sentrale forskningsinstitusjon og har som formål å drive forskning og utvikling for Forsvarets behov. Videre er FFI rådgiver overfor Forsvarets strategiske ledelse. Spesielt skal instituttet følge opp trekk ved vitenskapelig og militærteknisk utvikling som kan påvirke forutsetningene for sikkerhetspolitikken eller forsvarsplanleggingen.

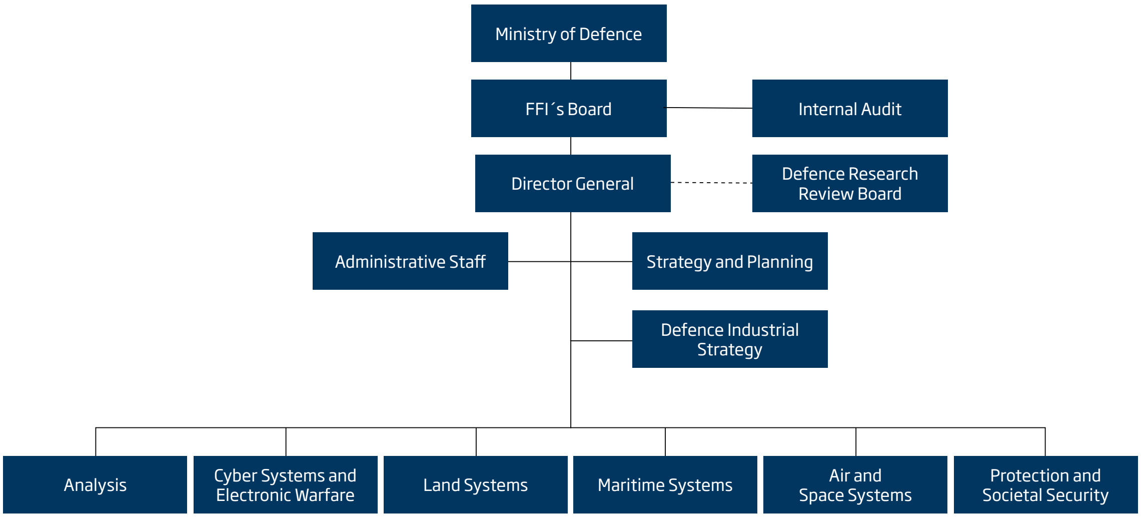
FFIs VISJON

FFI gjør kunnskap og ideer til et effektivt forsvar.

FFIs VERDIER

Skapende, drivende, vidsynt og ansvarlig.

FFI's organisation



Forsvarets forskningsinstitutt
Postboks 25
2027 Kjeller

Besøksadresse:
Instituttveien 20
2007 Kjeller

Telefon: 63 80 70 00
Telefaks: 63 80 71 15
Epost: ffi@ffi.no

Norwegian Defence Research Establishment (FFI)
P.O. Box 25
NO-2027 Kjeller

Office address:
Instituttveien 20
N-2007 Kjeller

Telephone: +47 63 80 70 00
Telefax: +47 63 80 71 15
Email: ffi@ffi.no

FFI Forsvarets forskningsinstitutt
Norwegian Defence Research Establishment