piql

A Risk Assessment of Piql Services

Extract by Piql of the report written by the Norwegian Defence Research Establishment

The following document is written by Piql AS.

It is an extract of the 174-page report "A risk assessment of the Piql Services" written by The Norwegian Defence Research Establishment as a conclusion to their thorough assessment of Piql Services. In addition, it contains an overview of measures Piql have taken to further minimize risk based on the recommendations in the report.

To read FFI's full report, please follow this link: https://www.ffi.no/no/Rapporter/16-00707.pdf

Contents

0 Preface

In one of Piql's ongoing research projects, PreservIA, - supported by the Norwegian Research Council, one of the tasks has been to make a detailed study related to a risk assessment of Piql's Services of providing ultra-secure data storage and long-term digital preservation. The aim of the PreservIA project is to further improve the Piql Services to better ensure the security, immunity and authenticity of the information stored on the storage medium, the piqlFilm.

The Norwegian Defence Research Establishment that has vast experience, and is a trusted authority globally on such risk assessments, was asked – and kindly accepted to perform this task in the project.

By performing a risk assessment to identify the Piql Services' vulnerabilities and security challenges, it has been established that it is the most appropriate method for preservation of digital data available today. The clearest benefit of the Piql Services is being a migration-free medium. This leads to saving resources, minimized risk for online manipulation or theft of data, and no manipulation, corruption or loss of data during a migration process.

Several theoretical worst-case scenarios reveal some vulnerabilities such as fire and the threat of an insider. These revelations offer Piql a chance to develop even stronger products and services, and thus distance themselves further from other migration based storage mediums in a positive direction.

Since the report "A risk assessment of the Piql Preservation Services" was published in June 2016, Piql have taken several measures to further improve Piql Services as proposed by the Norwegian Defence Research Establishment in their report.

This extract is a condensed summary of the 174-page report plus that it contains an overview of measures Piql have taken to further minimize risk based on recommendations in the report.

The assessment also functions as a guide for current and future Piql Partners since the report divides the world in three zones based on climate, development level and political stability. A Piql Partner can by determining which zone he belongs to, easily see which threats and hazards may threaten their production or storage facilities, and thus get an indication of what to include in their own risk and vulnerability assessments.

1 Introduction

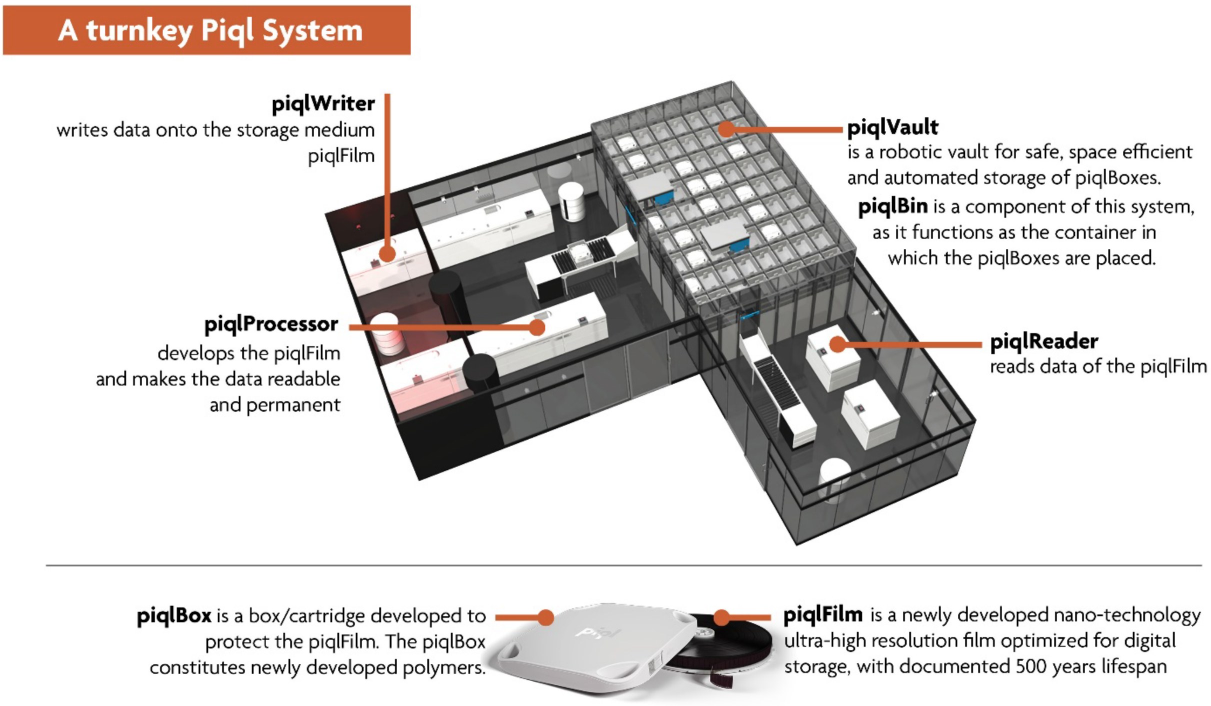
It was Aristotle who said "It is likely that unlikely things should happen". Only when we accept this, we can begin to plan for it. The purpose of this risk assessment has been to identify vulnerabilities and security challenges in order to be able to mitigate the effects they would have on the Piql Services. Identified risks will be analysed according to their effect on the confidentiality, integrity and availability of the preserved information. As the time frame for this assessment is 500 years, it is simply impossible from a scientific point of view to predict what changes our world will go through in that time. We have therefor dealt with trends and events we can perceive today. Note that the term 'risk' (rather than 'threat') includes both intentional acts and unintentional events.

The assessment is made through a scenario-based approach with a user-oriented perspective. Additionally, the report includes a brief overview of other digital storage technologies available in today's market, in order to place Piql Services in a wider context.

2 The Piql Services

The Piql System is a complete System for ultra-secure data storage or long-term preservation of digital data, that ensures data's authenticity, immunity and security for a timespan of over 500 years.

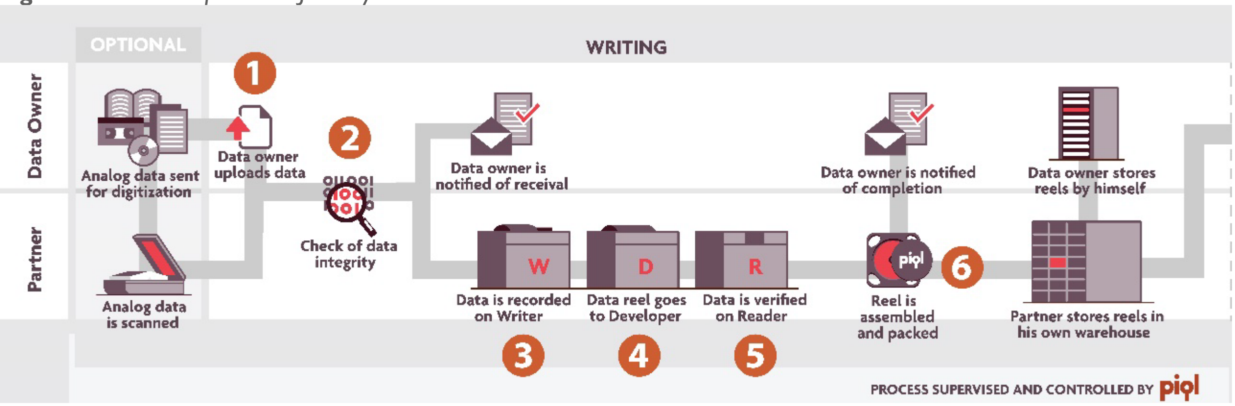
Figure 2.1: *An overview of the elements included in the Piql System.*
(This illustration has been added to this extract to give an easier understanding of the System as a whole)


A turnkey Piql System
piqlWriter writes data onto the storage medium piqlFilm
piqlVault is a robotic vault for safe, space efficient and automated storage of piqlBoxes.
piqlBin is a component of this system, as it functions as the container in which the piqlBoxes are placed.
piqlProcessor develops the piqlFilm and makes the data readable and permanent
piqlReader reads data of the piqlFilm
piqlBox is a box/cartridge developed to protect the piqlFilm. The piqlBox constitutes newly developed polymers.
piqlFilm is a newly developed nano-technology ultra-high resolution film optimized for digital storage, with documented 500 years lifespan

The Services provided by this System, reaches the market through selected Piql Partners located around the world. Every such Partner delivers these services to multiple data-owners in need of either ultra-secure data storage or long-term digital preservation across sectors and industries.

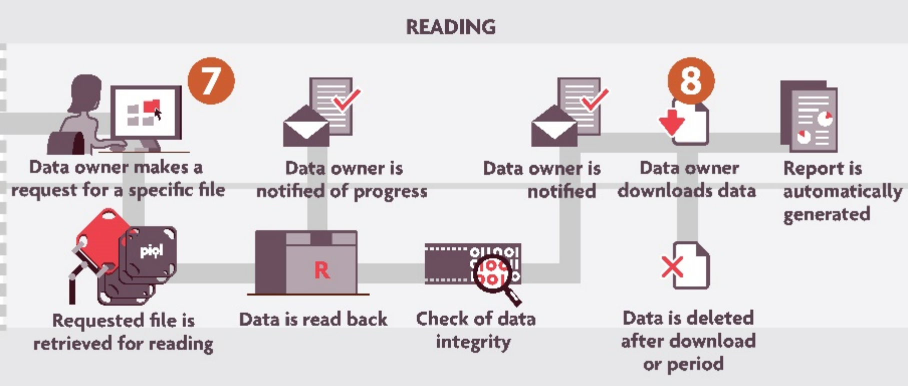
In order to gain a proper appreciation for how these Piql Services works, it is useful to go through the service journey (Figure 2.2) step by step to understand how visual data ends up on a piqlFilm in a secured storage facility.

Figure 2.2: The Piql Service Journey – Part 1


OPTIONAL
WRITING
Data Owner
Partner
1
Analog data sent for digitization
Data owner uploads data
2
Check of data integrity
Data owner is notified of receival
Data owner is notified of completion
Data owner stores reels by himself
Analog data is scanned
W
D
R
Data is recorded on Writer
Data reel goes to Developer
Data is verified on Reader
3
4
5
Reel is assembled and packed
6
Partner stores reels in his own warehouse
PROCESS SUPERVISED AND CONTROLLED BY piql

1. Digital born or digitized data is sent to a Piql Partner by a data owner.
2. When received, integrity checks are performed to make sure that the data was not altered during the reception, and also that no viruses etc. are transferred into the Piql System. The received data then goes through a preparation process with two purposes: to collect relevant metadata to enable future access to the data; and to encode both the data and metadata into the Piql System storage format, comprising a single file. Now the data owner has three choices: digital, visual or hybrid preservation of the data. Digital means that all the data is encoded to binary form. Visual means the data is printed as readable text or images. Hybrid is a combination of the two other options.
3. The data is then sent to the piqlWriter where it goes through yet another integrity check before being written to the piqlFilm. The piqlFilm is manually loaded into the piqlWriter by an operator who does not access the computer and thus the original file.
4. Once written, the piqlFilm is sent to a separate location for processing, before returning to the production site.
5. The content is verified by reading it back with the piqlReader.
6. Once verified, the original data is deleted from the computer system, and the piqlFilm is transported to a secure offline storage facility.

Figure 2.2: The Piql Service Journey – Part 2


READING
7
Data owner makes a request for a specific file
Data owner is notified of progress
Data owner is notified
8
Data owner downloads data
Report is automatically generated
Requested file is retrieved for reading
R
Data is read back
Check of data integrity
Data is deleted after download or period

7. Metadata from each individual piqlFilm is stored in an online database, where the data owner can search for any specific file and request retrieval.
8. The retrieved data can be sent to data owner electronically or in a physical form (e.g. hard drive).

The information stored on piqlFilm is self-contained. This means that regardless of available software or technology in the future, the data can always be retrieved. Instructions on how to retrieve the data is written in human readable text at both the beginning and the end of every reel of piqlFilm. If the data is written in visual format all you need, in theory, is a light source and a magnifying lens and you will be able to read it immediately. If the data is written in digital form, you also need a camera and a computer. Instructions on how to decode the frames back to readable files is included in the retrieval information mentioned earlier.

3 Scope

Risk assessments are a method to better manage risks; to be made aware of the threats and vulnerabilities towards our objectives makes it possible to put security measures in place. By having this assessment done at such an early stage, Piql ensures that the necessary modifications and manufacturing requirements can be implemented as early as version two of piqlFilm and piqlBox. Moreover, the security parameters surrounding the piqlVault can also be recommended to end users.

Value-oriented thinking is essential to this risk assessment and understanding the relationship between value, threat and vulnerability. In order to implement necessary security measures, it is necessary to be aware of the multitude of assets that will require protection, i.e. type of information and the corresponding sensitivity of that information. This could vary greatly: military secrets are for instance a lot more sensitive than a company's accounting records. The security level surrounding the Piql Services would vary in equal measure. The value of the assets will suggest what kind of threats they face and thus what their vulnerabilities are. The value-oriented thinking is therefore paramount to this assessment.

This risk assessment consists of three stages;

1. Risk identification:
   - mapping the object of analysis, the Piql Services
   - finding and describing corresponding risks

2. Risk analysis:
   - finding which intentional or unintentional threats/hazards is relevant to the different values-levels of the assets written on piqlFilm
   - the vulnerability of this value against said threat/hazard

3. Risk evaluation:
   - determining the level of risk
   - identifying security measures to reduce the harmful effect on the Piql Services

The processes or objects of study included in this assessment is:

1. The production phase
   - everything from the reception of data till the finished reel is placed in a piqlBox
2. The storage phase
3. The structures surrounding and connecting these objects
   - transportation between production site and storage facility
   - the operational processes of running the automated storage facility. Being a fully automated storage system, it relies on electricity to operate the robots that deposit and collect the piqlBoxes on requests made through the operational software, which in turn also needs electricity to function.

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 cause by one or more coincidences, i.e. unintentional events.
Security	Protection against unwanted events that are the result of deliberation and planning, i.e. intentional acts.
Risk	Expression of danger of loss of important values due to an unwanted event.
Threat	A possible unwanted event that can have negative consequences for the security of an entity. Used in this report in relation to an action performed by a threat actor, i.e. an intentional act.
Hazard	Source of potential harm. Used in this report in relation to an event without a deliberate cause, i.e. an unintentional event.
Vulnerability	Lack of ability to withstand an unwanted event or maintain a new stable state if an asset is subject to unwanted influence.
Risk assessment	Used here as a working definition: Overall process of risk identification, risk analysis and risk evaluation.

4.2 Terms related to Computer Security

Term	Definition
Information safety	Pre-emptive measures to secure confidentiality, integrity and availability of sensitive information throughout its existence. It is common to include measures to secure authenticity as well.
Confidentiality	The prevention of unauthorised disclosure of information.
Integrity	The prevention of unauthorised modification of information, i.e. the information is 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 unauthorised entity.
Authenticity	That the information is what it portrays itself to be. The property of being real and authentic.
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.
Information	The interpretation of data. Any form of intelligence in material or immaterial form.
Asset	The physical representation of 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. Used here as a synonym for the data stored on the piqlFilm in need of storage and protection.
Value	The assigned worth of an asset.

4.3 Terms related to the Scenario-based Approach

Term	Definition
Scenario development	The process of 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 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.

5 Simplifications and Specifications

5.1 Geography

Piql Services is a global organisation, and to divide the geography into more manageable groupings, the three geographical zones operated with in this assessment is North, Middle and South. This division is based on the following classifications; climate, development level and political stability. Climate was chosen as the main classifier, as it is deemed to be the most stable indicator over time, even considering climate change. Together these three indicators give an adequate description of the characteristics of a country. Climate gives relevant information about the geographical setting; development 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 geographical zones will serve to illustrate that a scenario plausible to happen at one location within a zone, can also easily happen in any other part of same zone. As a result of this assessment, a Piql Partner can by determining which zone it belongs to, easily see which threats and hazards may threaten their production or storage facilities, and thus get an indication of what to include in their own risk and vulnerability assessments.

***Figure 5.1:** Details of the indicators for the different zones*

Zone	Example regions	Climate	Developmental level	Political stability
NORTH	North America, Europe, East Asia (China, Japan)	***Temperate and subarctic***. Annual mean temp.: 10°C. Possible hazards: Earthquake, volcanic activity, flood, hurricane, tornado, tsunami, drought with extreme temperatures, blizzards, avalanche	***High.*** Strong economy, sophisticated infrastructure, stable energy supply, high standard on road network, sophisticated Ecom networks, high degree of law and order, proper crisis management. Possible hazards/threats: Loss of utilities, theft, espionage, sabotage.	***High.*** High degree of accountability to population, absence of violence/terrorism, high government effectiveness, rule of law, control of corruption, very stable borders. Possible threats: Terrorism, insider theft in low-scoring countries.

Zone	Example regions	Climate	Developmental level	Political stability
MIDDLE	Northern Africa, Middle East, Indian subcontinent	***Subtropical*** Annual mean temp.: 25°C Possible hazards: Sand storms, extreme temperatures, flood, hurricane, volcanic activity, earthquake	***Medium/low*** (yet pockets of higher levels within countries) Weak economy, poorly developed infrastructure, highly unstable energy supply in certain countries, 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, loss of communications, theft.	***Low*** Low degree of accountability to population, incidents of violence/terrorism, low government effectiveness, little rule of law, poor control of corruption, potentially unstable borders. Possible threats: Unstable borders, war, terrorism, theft.
SOUTH	South America, Southeast Asia, Southern Africa, Australia	***Tropical*** Annual mean temp.: 20°C Possible hazards: Flood, hurricane, extreme temperatures, earthquake, volcanic activity	***Medium*** Growing economy, adequate infrastructure, adequate energy supply, medium transport networks, adequately developed Ecom networks, good degree of law and order, ok crisis management. Possible hazards/threats: Loss of utilities, loss of communications, theft, espionage, sabotage	***Medium*** Medium degree of accountability to population, some incidents of violence/terrorism, adequate government effectiveness, low rule of law, problems with control of corruption, stable borders. Possible threats: Terrorism, theft

6 Scenario method

6.1 Unintentional events

To categorize all unintentional events which could affect a nation's security, a modified version of morphological analysis has been utilised, where the only two parameters were *cause* and *primary effect.*

Figure 6.1: *Matrix for analysis of scenario classes of unintentional events*

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	

Based on the causes and effects outlined above, the following scenario classes in the category of unintentional events has been identified: natural disasters, failure or malfunction, sudden illness and aggregated individual acts.

The two latter – sudden illness and aggregated individual acts – are deemed not relevant because the risk they pose to the Piql Services are too implausible or irrelevant for its safety and security.

The two former scenario classes – natural disasters and failure or malfunction – are more plausible and relevant. Below are the listed events included in these two classes:

Natural disasters:

Meteorological events:

- Extreme winds
- Extreme temperatures
- Different grades of precipitation
- Flood

Geological events:

- Earthquake
- Volcano eruption
- Tsunami
- Avalanches

Cosmological events

- Meteor showers
- Radiation

Failure/malfunction:

Harmful emission:

- Chemical
- Biological
- Radioactive

Conventional accidents:

- Explosions/fire
- Structural collapse
- Transport accident

Cosmological events

- Meteor showers
- Radiation

6.2 Intentional acts

To categorize all **intentional acts** that could threaten the Piql Services directly or indirectly, the following parameters has been defined:

Figure 6.2: *Matrix for analysis of scenario classes of intentional acts*

Actor	Goal/purpose	Method	Means
State	Political power	Physical destruction	Conventional weapons
Network	Market power	Physical manipulation	Non-conventional weapons
Company	Economic gain	Logical destruction	Hand or power tools
Individual	Personal interest	Logical manipulation	Malicious transmitters
		Inside	Software tools
			Monetary means

Having done a qualitative evaluation of the possible scenarios to come out of this matrix, the following scenario classes has been deemed relevant to the Piql Services;

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 piqlFilm with sensitive information for use other than selling film directly

Espionage:

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

Terrorism

- As revenge on data owner
- piqlFilm as collateral damage

Nuclear war:

- piqlFilm as collateral damage

Sabotage:

Of the structural integrity of the building housing the storage facility

- Physically damaging the structure
- Physically damaging the security barriers

Of the piqlVault system:

- Physically damaging the components of the piqlVault system
- Logically malware EWMS to create chaos in the system
- Jamming/altering radio signals

Of the Piql System production

- Malware that alters information during preparation for writing
- Physical damage to the piqlWriter and piqlReader

Of the piqlFilm

- Physically damaging the piqlFilm

Armed conflict

- piqlFilm is the target of a coordinated attack

6.4 Final selection of scenarios

Based on the scenario classes produced by the matrixes of both intentional and unintentional events, the following selection of scenarios has been made:

- **Accident:** an unfortunate incident that happens unexpectedly and unintentionally.
- **Technical error:** can cause cease of operations or functionality in a system.
- **Natural disasters:** a sudden natural accident or catastrophe that causes great damage.
- **Crime:** a serious offence against an individual or a state, and is punishable by law. It can be politically motivated, economically motivated or simply due to a wish to inflict pain.
- **Sabotage:** Intentional destruction, shut down of equipment, materials, facilities or activities. Intentional disarmament of persons executed by or for a foreign state, organisation or group.
- **Espionage:** Gathering of information using secret means in an intelligence capacity.
- **Terrorism:** Illegal use of, or the threat of use of, force and violence against persons or property in an attempt to place pressure on a country.
- **Armed conflict:** Conflict between states or groups that involves use of armed force.
- **Nuclear war:** A warlike state in which the main means are weapons of mass destruction.

The final step of the morphological analysis method used in this assessment, is to describe specific scenarios in detail. The number of scenarios chosen to be part of this assessment is abnormally large, as the risks and threats which may harm the Piql Services are so many.

8 Presenting the Scenarios

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.

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 either. The sparks cause an electrical fire at the charging stations at the top of the grid which spreads. The fire sets of 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.

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 waterproof 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 no one without authorized 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.

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, were saved.

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.

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.

Scenario 7 also presents the theft of sensitive information, though in this scenario the threat actor is an organized 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.

Scenario 8 presents sabotage, a very relevant threat to the Piql Services. State X hackers are able to perform logical sabotage on the client information which is being prepared for writing. The hackers place malware in the system which utilizes 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.

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 66 FFI-RAPPORT 16/00707 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.

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.

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 unauthorized 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.

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.

9 The Vulnerabilities and Security Challenges of the Piql Services

Before the risks faced by the Piql Services are described, it must be stressed that the assessments made here are purely theoretical and the results have not yet been practically tested. It is also important to keep in mind that the higher sensitivity of the information stored on the piqlFilm, the higher potential value it has for a threat actor. Having the right security and safety measures then becomes even more vital than if the piqlFilms stored less valuable information.

9.1 Vulnerabilities and Security Challenges identified

We start by describing some general risks to the Piql 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"

The piqlFilm is always more vulnerable when it is "out in the open". This statement refers to both when the piqlFilm is outside the piqlBox (production & readback) and when the piqlFilm is outside a Piql-controlled environment all together. When in production or storage 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. But when in transportation the measures put in place are fewer and factors outside of the Piql partner control are more numerous.

9.1.2 Inside threat

One of biggest security challenges to the Piql Services identified is the inside threat, or "the insider". Such an insider can act of their own volition, motivated by the prospect of revenge, or they can act on behalf of someone else, possibly if they have received a bribe. The insider can also be forced to somehow harm the Piql Services, for example if they are the subject of extortion. In the earlier stages of the Piql Services Journey an insider is in a position to damage the piqlFilm physically, he can remove the piqlFilm altogether or he can steal original files which would compromise the confidentiality of the information. Once the piqlFilm is in storage these acts become more difficult. In choosing an automated storage system, a pick-up must be ordered electronically and would thus leave a record of the transaction.

9.1.3 Loss of Ideal Storage Conditions

This can be caused by either loss of utilities causing ventilation systems to stop working, or by damages to the infrastructure of the building which houses the Piql Services causing outside air to flow into the storage facility. Energy supply is vital to maintain stability of the storage facility. Piql AS stipulates that all piqlVaults must have a power generator in case of power outage, but other than this small measure the Piql Partners are vulnerable to events that can affect their power supply.

In order for the 500-year longevity to be guaranteed, the storage conditions must be kept at no higher temperature than 21 °C and no higher humidity than 50%. This means that higher level than normal will cause more damage than lower levels.

If, however, they get too low, this may cause some changes to some of the mechanical properties of the piqlBox and piqlFilm, and make them more brittle. The negative effects this can have on the piqlFilm can fortunately be avoided simply by letting it thaw under controlled conditions. Piql AS has executed extensive tests to this effect., where the piqlFilm has been stored in a Cryotank at -196 °C for 24 hours before being defrosted under controlled conditions. When data has been read back from these piqlFilms, there were little signs of damage.

High temperatures and humidity can cause the piqlFilm to warp because of shrinkage along the edges, which in turn can affect the readability. Tests conducted by Piql also shows that high humidity gives a possibility of blemishes growing the film as well as fungi. However, the increased level of temperature and humidity required for negative effects to occur are quite high. The piqlFilm can withstand temperatures up to 85°C at a relative humidity of 50% for up to 23 weeks before it affects the readability of the piqlFilm. The materials used in the Piql components are supposed to withstand quite a lot when it comes to changes in temperature and humidity when it comes to shorter exposure.

9.1.4 Fire

Fire is a major risk to the integrity of the piqlFilms. In a regular room fire, where temperatures can reach between 600 and 1200°C, some piqlBoxes and Films will be devoured by the flames, whereas others will simply be exposed to excessive heat.

The piqlBoxes that come in contact with fire, will burn and melt. At a 170°C the once hard plastic, will turn into a thick sticky mass. When this in turn comes in contact with the content of the piqlBox, the piqlFilm, it will compromise its integrity.

If the piqlFilm itself is touched by the fire, even though the polyester base is slow-burning with enhanced resistance to heat, it cannot withstand flame temperatures. The integrity of the piqlFilms that are only exposed to the heat of the fire, however, stands a very good chance of remaining intact as it is proven to withstand 121°C for 24 hours without significant loss in readability.

9.1.5 Water

Although there has not been conducted proper testing on the effects of water on the piqlFilms, it is easy to assume that it would be a major risk, perhaps even more so than fire, to the Piql Preservation Services.

We do have valuable input of the consortium partners that both the PP (i.e. the polymer material Polypropolene) of the piqlBox and the PET (Polyethylene terephthalate) of the piqlFilm is very water resistant. Both plastics can be submerged in water a very long time without showing notable changes. However, this makes no mention of the quality or temperature of the water, and in case of a flood, where the water would be filthy, of a higher temperature and acidic or basic, we can safely assume that the piqlFilm would be damaged beyond repair.

For the piqlVault, whose operation entirely consists of electronics, the water is obviously very damaging. The system would short-circuit and shut down and manual recovery of the piqlBin would then be necessary.

9.1.6 Physical pressure from overhead weight

How the piqlBox and piqlFilm can withstand different degrees of physical pressure before being damaged beyond repair, is a risk that requires more testing. Naturally, they will be crushed if hit by big pieces of concrete in case of an earthquake. However, smaller pieces of concrete will not crush everything they land on, but simply add more weight to what's underneath them.

The piqlBoxes are said to withstand an impact of 5 Joule, which is deemed to be quite modest. The piqlFilm we can assume holds an advantage in the way it is tightly rolled into a coil.

9.1.7 Jolts and Drops

Initially, this was deemed a major problem for the Piql Services. Human error or external force could lead to the piqlBox being dropped to the floor, and the piqlFilm could fall out and be damaged. The Library of Congress in the US has specified a drop test requiring that a container must be able to drop from a height of 180 cm while containing a full role. The piqlBox fails this test today, but future versions aim to comply with this test.

However, an automated storage system makes a substantial difference in this case, with minimal handling by human operators needed and the tight stacking of the piqlBins within the grid.

9.1.8 Chemical Compounds

Acid and bases have no or only minor effects on the piqlBox, but strong oxidative chemicals, like ozone, will lead to reduced longevity. Though for the negative effects to become evident, high temperatures (60°C) and more humidity are needed.

Contrary to the piqlBox, the piqlFilm is very susceptible to negative effects of chemical gasses. And as the piqlBox is not air-tight, the gas will come in contact with the piqlFilm. The weakest link is the gelatin in the emulsion layer of the piqlFilm, it will completely dissolve at very little exposure. And as with the piqlBox; with higher temperatures and humidity the effects are worsened.

9.1.9 Harmful Microorganisms

Even though there is no scenario describing how the Piql Services handles harmful microorganisms, it is important to include, especially as the reactions of the piqlBox and piqlFilm when exposed to this, are quite similar to when being exposed to chemical compounds. Being a protein, the gelatin in the emulsion layer of the piqlFilm, is biodegradable.

9.1.10 Nuclear Radiation

If located within the reach of the destruction caused by the explosion itself, the Piql Services will be annihilated along with everything else. But if located out of reach of the destruction caused by the detonation, but exposed to maximum amount of radiation, the piqlFilms would suffer high-energy radioactive fallout over a long period of time.

Although the plastic materials in both piqlBox and piqlFilm will react to this exposure, it will not do so to the extent one might expect. Both the PET and the gelatin on the piqlFilm will weaken, but the effects are barely significant. The piqlBox will become brittle and loose its flexible strength. The radiation alone will not compromise the readability of the data. However, being located this close to the blast, the air pressure, the heat wave or the firestorm following a nuclear blast will most definitely destroy them.

If the distance to ground zero is such that the air blast and firestorm does not destroy it, the piqlFilm should survive.

9.1.11 Electromagnetic Radiation

Electromagnetic radiation, or electromagnetic impulses (EMP), will have no influence on the piqlBox or piqlFilm. These impulses can destroy electrical equipment, but will have no effects on plastics.

The electronic security measures in and around the piqlVault on the other hand, will be effected. All operations will cease, which in turn compromises the availability of the piqlFilms as repairs to the electronics of the piqlVault system must be undertaken before it can operate again.

9.1.12 Ultraviolet Radiation

Under normal storage conditions the piqlFilm is coiled and placed in a piqlBox, and these packaging features should both protect the piqlFilm from exposure to UV radiation.

However, if a scenario should occur where the piqlFilm is left out in the sunlight, the silver halides in the emulsion layer of the film will be bleached, and the information cannot be read back and hence will be lost.

9.1.13 Theft

As a storage medium of potentially very valuable and sensitive data, theft is one of the biggest threats to the Piql Services as well as one of the more consistent ones in this 500-year risk assessment.

Logical theft would mean stealing the information while it is stored or electronically transferred. Physical theft would mean stealing the physical storage medium. As the piqlFilm is a migration free, offline medium, the need for contact with online networks is limited to the production phase. The risk of logical theft is thus few. On any other point of the service journey, a threat actor would have to physically remove the entire piqlFilm. The greatest risk for this happening is during transportation, but also plausible during storage. Once again though, by choosing an automated storage system, the risk of theft during storage would be mitigated.

9.1.14 Sabotage

Sabotage is another major concern for the Piql Services, both in terms of damaging the information itself, but also to simply create chaos. Both which could compromise the integrity and availability of the information. Sabotage can primarily take place in two phases; production and storage. And as with theft, there is a distinction between logical and physical sabotage, i.e. damaging or altering the information while its electronically transferred, or damaging the physical entities and surroundings of the Piql Services.

During storage, a threat actor could affect the availability of the piqlFilms by gaining access to either the Piql IT system or the radio signals that controls the robots in the automated storage system. However, the main risks of sabotage during storage are of a physical nature. The building housing either the production or storage facilities, or the energy supply can easily be targeted by a threat actor and thus affect the availability of the stored information.

During production, the machines can be the targets for physical sabotage, but this would only delay the production and not threaten the integrity or availability of the information. Logical sabotage can on the other hand do some real damage during this phase. A threat actor with the right skills can access the Piql IT system and alter or delete the information.

Finally, the piqlFilm itself can suffer from physical sabotage at any point of the service journey. An insider or someone else who gains access to the piqlFilm can either cut away frames or scratch the entire length of film, to where the information would be impossible to read back.

9.1.15 Espionage

This risk becomes present when the information stored on the piqlFilm holds great value to a threat actor, and it would have to take place in the production phase when the information is still connected to online networks. A threat actor with the right skills could install spyware in the Piql IT system, and thus access the information. The integrity of the information would remain intact, but the confidentiality would be grossly compromised.

Espionage can of course also include to physically get hold of the piqlFilm, but this action has been put under theft in this assessment.

9.1.16 Threats to Computer Security

Though the security mechanisms demanded of the Piql Partners by Piql AS are relatively strong, there are three weak points that must be considered in the Piql IT system.

Firstly, because of the constant evolving software solutions and the 500-year perspective of this assessment, it is nearly impossible to analyze the reliability of the security software employed in the Front-End service. 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.

Secondly, a threat actor holding formidable hacking skills can gain access to not just the computer connected to the outside world used to receive and process information, but the entire Piql computer system. This will give the threat actor the possibility to alter the checksums used to verify that the information received is the same as the information being printed to the piqlFilm. The client data is thus no longer safe from attacks on its integrity.

The third weakness in the Piql IT security architecture, is that cryptographic protection is not provided. To keep with the principle of 500-year longevity, Piql wants the information stored on piqlFilm to be self-contained and if it is crypted, future access cannot be guaranteed without additional references. However, this trade-off between security and self-containment should be up to the user to decide. The decision depends on whether the user values availability or confidentiality the most. So, by not offering cryptographic protection, the information security setup is deemed weak.

Apart from these three weaknesses, there are some worth mentioning regarding the piqlVault IT system. As mentioned previously, a threat actor can create chaos with regards to the locations of piqlBins and thus affect the availability of the information. He can do so by accessing the piqlVault IT system and switch the reel ID's around, or by affecting the radio signals controlling the robots.

10 Alternatives for Digital Storage

10.1 Existing Digital Storage Technologies

10.1.1 Hard disk drive (HDD)

This has been the main form of data storage in computer systems for decades, and offers a cost efficient and easy accessed way to store and retrieve data. The maximum storage capacity is 10 TB per disk. A human hair, a dust particle or even a fingerprint can block the transformation of information from the write head to the disk, which means the failure rates are high, and thus makes this an inappropriate medium for long-term preservation. Due to short lifespan and these high failure rates, it is common practice to make use of several disks to ensure data redundancy and minimize the risk of data loss.

10.1.2 Optical disk

This is a flat circular disk that encodes digital data, and is most commonly used for distribution and storing of software, games, audio- and video-recordings. The CD-R and DVD-R versions writes information only once and thus the information stored is immune to corruption for the longevity of the medium. The CD-RW and DVD-RW however, allows new information to be rewritten onto the same medium.

This medium offers low capacity with a maximum of 700 MB for CDs, 8,4 GB for DVDs and 50 GB for Blue-ray, and a relatively short lifespan of 2-5 years. They are a fragile medium that may snap or scratch easily, and is affected by dust, heat and UV light.

10.1.3 Magnetic tape (LTO)

This medium stores visual files on a narrow strip of film with a thin magnetisable coating. To find and retrieve information stored on LTO is time-consuming, it is therefore most appropriate to use this medium for data that will not be needed instantly. If the LTO is placed near a strong magnetic field e.g. a large speaker or a magnet, the data stored on the tape may be corrupted.

The lifespan is up to 30 years, but really this only applies if information is stored and hardly ever accessed again. If the added wear and tear of regular use is added, a more realistic lifespan is about 10-20 years. Still, the best practice for storing information on this medium is to migrate the data every 5-10 years.

10.2 Security Qualities

Comparing these technologies to Piql Services, it is safe to say they would not be able to withstand the negative effects of the worst-case scenarios that has been outlined in chapter 8. They would all be vulnerable to excessive heat, filthy water, physical pressure, chemical compounds, harmful microorganisms, the insider threat and sabotage. Radiation, however, differentiates the different mediums. Electromagnetic radiation has no effect on an optical disk, but will highly effect the information stored on HDD or LTO. The reverse is true when it comes to UV radiation; HDD or LTO will not be affected, but damage can be done to the information stored on optical disks when exposed to too much sun or overhead lights.

10.3 Long-term preservation

When it comes to preservation of digital data – understood as maintaining something in its original state, keeping it alive and safe from harm – the Piql Services is the most appropriate storage method available today. Using this migration free solution, a client can save a lot of resources both in terms of cost, storage infrastructure and labour. The longevity of the piqlFilm removes the risk of data being lost, manipulated or corrupted during migration. And finally with no need for migration means the information is not connected to external networks for longer than strictly necessary. This minimizes the chance for a threat actor to manipulate or steal data.

11 Recommendations

General recommendations on security measures are made so that the Piql Partners can keep the piqlFilms they store as protected as possible. However, it is important to remember that there is no "one size fits all" in this matter. Different geographical settings, market areas, sectors and level of sensitivity play important roles, so it is up to the individual users how to prioritize the risks uncovered by this assessment. Additional recommendations are then made for the Consortium partners of alterations to the Piql components, which they may decide to implement in future versions.

11.1 Recommendations for General Security

A general rule of information security is to always keep backups. One should therefor request more than one copy of piqlFilm, and they should preferably be placed in different locations. Another general measure to employ is to preserve the information using the hybrid method, i.e. both as visual text/images as well as digital.

It has previously in this assessment been stated that the piqlFilms are at their most vulnerable during transportation. Changing the transportation route from day to day would make it more difficult for a threat actor to stage an assault, but having the production site at the storage facility would remove the entire risk altogether.

The insider threat was highlighted as one of the biggest security challenges the Piql Systems faces. To mitigate this risk, one can:

- Have sound procedures like security clearance, check of criminal records, and credit check in place during hiring processes.
- Perform such checks at regular intervals during employment.
- Make sure only a few highly trusted people have access to the most critical parts of the service.
- Implement control system where a second Piql operator needs to approve that a piqlFilm is withdrawn from the storage system or leaving the storage facility.
- Ensure that a person never works alone, that being an operator of the production or a security guard working the nightshift.

11.2 Recommendations for Physical Security

One event that can cause loss of ideal storage conditions is loss of utilities, most importantly; energy supply, but also water, gas etc. Backup generators and doubling of energy supply from two independent sources, f. ex electricity and diesel, is recommended.

In case of fire inside the building of where the piqlFilms are stored, vast supply of oxygen retricting gas is important. A sprinkler system can potentially do more harm than the fire it is meant to put out. If the fire is outside of the building, i.e. a forest fire, measures needs to be taken on the construction of the building and its surroundings, such as clearing a safety zone between structures and vegetation, and only using fire-resistant or non-combustible materials on exterior surfaces. It is also a recommendation to add some sort of flame deterrent to the piqlBox itself, to mitigate the risk of damaging the piqlFilm in case of a fire.

Since there is not sufficient information to make a clear statement regarding the effects of water on the piqlFilm and piqlBox, the recommendation to the Consortium partners is to conduct tests of the piqlFilm with both clean, dirty, hot and cold water, with different duration of submersion. Despite this lack of information, it is still recommended to avoid exposure of the piqlFilm to water, to prevent the film layers sticking together, and the swelling and softening of the emulsion. A preventive measure would be to develop an air-tight i.e. waterproof piqlBox.

How the piqlBox and piqlFilm is effected by jolts, drops, and external physical pressure, f.ex. falling infrastructure due to an earthquake, is another subject with the lack of information. Similar to the case of water effects, we recommend that tests be conducted to better understand the consequences of such events.

In chapter 9 we described how strong oxidative chemicals, like ozone, would cause great damage to the piqlFilm, but also the piqlBox. A possible solution would be to wrap the piqlBox in a sealed aluminium foil to ward off gasses, as well as bacteria and other microorganisms. This type of measure would also mitigate damages to the piqlFilm caused by water.

In terms of nuclear radiation and electromagnetic radiation, we make no specific recommendations. The likelihood of nuclear radiation effecting the Piql Preservation System is too low to make radial changes to the safety and security measures. If electromagnetic radiation was ever directed specifically at the Piql Preservation Services, the technology would be negatively affected for a time, but the confidentiality and integrity of the stored information would remain intact. Ultraviolet radiation on the other hand can affect the integrity of the information stored on piqlFilm quite severely. We therefor recommend to never leave the film exposed to sunlight, and to use appropriate lighting inside.

When it comes to physical theft and physical sabotage, we recommend to ensure a sophisticated security regime is in place in and around both production and storage facilities in the form of fences, camera surveillance, alarm systems and employed guards both during and outside of office hours.

11.3 Recommendations for Computer Security

We recommend that the guidelines set forth by the Norwegian National Security Authority[1] to ensure the most impenetrable computer security regime, must be in place. These stipulate: all hardware and software

[1] Read the full 10 recommendations in the appendix.

must be state of the art, update security software as fast as possible, never distribute administrator rights to end-user, and block any unauthorized programs. Studies show that these four measures stop 80-90% of all internet related attacks. In addition, the guidelines say to activate code protection against unknown vulnerabilities, harden applications, utilize firewalls on client interfaces, use secure booting and hard disk cryptography, use anti-virus and anti-malware, and never to utilize more applications than strictly necessary.

In addition, we recommend Piql AS to offer its users cryptography at the Front-End service before information is transferred, and also to implement cryptography for protection of the information after it enters the Piql IT system. Though it would compromise the vision of being self-contained, whether this feature should stay intact or not should be up to the individual user to decide.

12 Conclusions

The vulnerabilities and security challenges identified in this assessment may seem numerous, but as absolute worst case scenarios have been included, in reality the outlook is not so grave. Many of the problems also have easy solutions.

The scenario analysis identified several vulnerabilities, some severe; such as fire and the threat of an insider, and some not so severe; like electromagnetic pulses and nuclear radiation, and some that simply require more testing.

The main finding in terms of vulnerabilities, is that it is the gelatin emulsion layer of the piqlFilm that is the weakest link, and as this is where the information is written, this vulnerability could have grave consequences for the security of the information stored. However, the gelatin silver print method has been used to preserve photos and moving images since 1874, and despite imperfect storage conditions, some of the first examples still exists today.

Nevertheless, Piql Services has many strengths. For example, the choice of materials, disregarding the gelatin emulsion layer, 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, seems to withstand a great deal of external influence.

A choice of an automated storage facility has enhanced the security and safety of the Piql Services. The modified piqlVault system may eliminate many risks: the tight stacking of the piqlBins strengthens the stability, it is more difficult for an outsider to access the stored information and it decreases the chance of human errors in terms on handling the piqlBoxes.

Perhaps the most significant strength is that the piqlFilm is an offline medium. And with 500-year longevity, meaning no need for migration, it sets Piql Services apart from any other physical storage medium for digital information. The content-data is only connected to online networks once, and only a handful of people must be involved. The number of potential risk sources eliminated is therefor great. And even when connected to online-networks, the computer security mechanisms put in place by Piql AS are relatively strong.

When it comes to physical security there are some issues in terms of forces outside of ones control, be it forces of nature or threat actors with malicious intents. Taking necessary precautions and constantly being aware of potential risks should be sufficient. With time the level of risk may be made even lower if alterations as a result of this assessment. Ultimately, the decision to store information in any manner is a matter of risk acceptance. There will always be risks involved with every storage system when valuable information is involved. It simply a matter of placing the risk at a level acceptable to the user.

13 Appendix

13.1 Recommendations by the Norwegian National Security Authority

The Norwegian National Security Authority

Ten important measures against cyberattacks

Step 1: The four most effective measures

1. **Upgrade software and hardware.** Newer versions of software/hardware will seal more security holes than older versions, and they often have better security features.
2. **Install security updates as soon as possible.** Even the best products have flaws and vulnerabilities which could be exploited by attackers. System owners should establish a centrally controlled regime for update of applications, operating systems and firmware (f. ex. BIOS code).
3. **Do not assign admin rights to end users.** Most end users do not need administrator privileges. In a centrally managed system, end users get the software they need from a common distribution point.
4. **Block running of unauthorized programs** ("whitelisting"). Use tools such as Windows AppLocker to verify that end users only run approved applications. Block special programs outside the approved folders and removable media, such as on CDs and memory sticks.

Studies show that these four measures stop about 80-90% of Internet-related attacks.

Step 2: Six additional measures

5. **Activate code protection against unknown vulnerabilities.** DEP SEHOP, ASLR and EMET forces the system against vulnerabilities in applications and operating system even when there's an update
6. **Curing applications.** Protected Mode / View for Internet Explorer, Microsoft Office and Adobe Reader limiting the extent of the compromise. Disable unnecessary mobile code and macros.
7. **Use client firewall.** Windows Firewall blocks all unsolicited incoming traffic and logs safety related events. Inspect the log files regularly.
8. **Use secure boot and disk encryption.** Windows Secure Startup and Windows BitLocker uses measurements and hard drive encryption to detect tampering of the boot process and prevent data loss from stolen / lost PCs.

9. **Use antivirus / anti malware.** Antivirus detects and blocks known malware which i.a exploits vulnerabilities in email applications and document readers. Preferably, one should use a product that can be centrally managed and that works well with the operating system.

10. **Do not install more functionality than necessary.** Any new application and function increases the possibilities of attack. Few users for example needs Java Runtime or JavaScript in Adobe Reader. Also, unnecessary software must be cured and updated, increasing the administrative burden on the system.

13.2 Identified threats & hazards – comments/measures taken by Piql

Threat/hazard		Details	Consequence	Recommendations by FFI	Comments and Measures taken by Piql
Fire	Room fire	Direct contact with flames, or exposure to heat for short period of time.	piqlFilm & Box that comes in contact with flames will burn & melt. piqlFilm that is merely exposed to the heat stands a good chance of surviving.	Oxygen restricting gas.	Detailed instructions on fire preventive measures (including the requirement of oxygen restricting gas), is a part of the requirements for the infrastructure of a piqlValt (storage facility) that we require all Piql Partners to comply with. Further Piql is in the process of establishing the Arctic World Archive, an ultra-secure mountain vault on the arctic island of Svalbard.
	Technical fire	As above. In addition; electrical systems will shut down.	As above. In addition; piqlVault will shut down and leave the piqlBoxes unavailable.	As above. In addition: sprinkler system should not be present in the storage facilities, as it can cause more harm than the fire it is meant to put out.	
	Forest fire	Direct contact with flames, or exposure to extreme heat for a long period of time.	piqlFilm & Box will burn and/or melt unless the location of storage has extensive fire protecting measures installed.	Clearing a safety zone between structures and vegetation and only using fire resistant and non-combustible materials on exterior surfaces.	
Water (needs more testing)	Sprinkle system/fire hoses	Spraying from the top down, splashing the upper layers of piqlBoxes and potentially submerging the lower levels.	The piqlFilm submerged in water will most likely be destroyed as the piqlBox is not waterproof. If recommended drying procedure is followed, it can be saved.	Recommend developing an air-tight i.e. waterproof piqlBox. Also recommend further testing of the piqlFilm with both clean, dirty, hot and cold water, with different duration of submersion.	We have created an airtight and waterproof "wrapping" of laminated foil with a layer of aluminium to be sealed around the piqlBox. This eliminates the problem with potential intrusion of water into the piqlBox. This foil has been tested with respect to longevity properties, and will not affect the longevity of the piqlFilm.
	Extreme flood	piqlFilm & Box will be submerged in filthy water full of debris, potentially holding a high temperature.	As above, but debris may cause piqlBox to open, filth in the water may scratch the film, warm water may affect the emulsion layer of the film.		
Jolts & drops		Human error or earthquake causing piqlBox to fall to the ground.	The piqlBox opens and the piqlFilm falls out, allowing it to be scratched, damaged and potentially exposed to damaging light, warm temperatures or humidity.	Recommend further testing to better understand the consequences of such events.	Early 2017 a significantly a better locking mechanism between top and bottom of piqlBox has been introduced. This will ensure that the piqlBox can withstand a free fall from 1,2 meter (operational height) without opening.
Chemical Compounds	piqlBox	Acid, bases and strong oxidative chemicals (i.e. ozone).	Acid and bases have no or only minor effects. Ozone can reduce longevity in high temperatures (60°C).	Possible solution would be to wrap the piqlBox in a sealed aluminium foil.	The airtight and waterproof "wrapping" of laminated foil to be sealed around the piqlBox eliminates the problem with potential intrusion of acids, bases and oxidative chemicals into the piqlBox and consequently the piqlFilm.
	piqlFilm	Acid, bases and strong oxidative chemicals (i.e. ozone).	Because the piqlBox is not air-tight, the gas will come in contact with the piqlFilm, causing the emulsion layer to potentially dissolve.		
Harmful Microorganisms	piqlBox		piqlBox will have no or only minor effects from harmful microorganisms.	Possible solution would be to wrap the piqlBox in a sealed aluminium foil.	The airtight and waterproof "wrapping" of laminated foil to be sealed around the piqlBox eliminates the problem with potential intrusion of microorganisms into the piqlBox and consequently the piqlFilm.
	piqlFilm		Being a protein, the gelatine in the emulsion layer, is biodegradable and will dissolve if exposed to harmful microorganisms.		

Threat/hazard		Details	Consequence	Recommendations by FFI	Comments by Piql
Nuclear Radiation	In reach of explosion		Everything will be destroyed.	The risk of this happening is deemed to low to make any radial changes to safety and security measures.	Piql is planning a project where this will be tested in depth. Further Piql is in the process of establishing the Arctic World Archive, an ultra-secure mountain vault on the arctic island of Svalbard.
	Exposed to radiation		The piqlFilm will weaken, but with barely significant effect. The piqlBox will become brittle and loose it's strength.		
Electromagnetic Radiation	piqlFilm & piqlBox	Electromagnetic pulses (EMP)	Will have no effect on neither the piqlFilm nor the piqlBox.	If EMP was ever directed at the Piql Preservation Services, the technology would be negatively affected for a time, but the piqlFilm and piqlBox would remain unharmed.	No further action needed.
	piqlVault	Electromagnetic pulses (EMP)	All operations will cease, and repairs to the electronics must be undertaken before it can operate again. The availability of the piqlBoxes is compromised.		We have a back-up system with no connection online. Since there is little urgency in what we do, seize of operations for some time is not necessary a problem.
Theft	Logical theft	Stealing information whilst it is electronically available	As a migration free, offline medium, the need for contact with online networks is limited to the production phase. The risk for logical theft is thus low.	No further action needed.	We recommend that the production site and the storage facility is under the same roof. If transportation is needed, a background check of driver will be performed and the driving routes will be alternated to reduce predictability of transportation route and incidents to occur.
	Physical theft	Stealing a physical reel of piqlFilm	The transportation offers the highest risk of physical theft, but it can also happen during storage.	Change route of transportation from day to day, or have the production facility and the storage facility at the same location. Ensure a sophisticated security regime is in place.	
Sabotage	Logical or physical sabotage of stored information.	Logical sabotage would have to take place whilst information is electronically available. Physical sabotage can also take place during storage.	Can delete or alter stored information, or physically damage the piqlFilm.	Ensure a sophisticated security regime around the production and storage facilities. Follow the guidelines set forth by Norwegian National Security to ensure the most impenetrable computer security regime	Piql is following the guidelines on computer security set forth by Norwegian National Security. Thus the risk of someone hacking into our systems to perform sabotage is reduced to almost non-existing. No Piql-employee can access the entire Piql Service Journey, which also minimise the risk of insider performing such sabotage.
	Creating chaos		Can i.e. alter reel ID's in the Piql IT system or target energy supply.	Follow the guidelines set forth by Norwegian National Security to ensure the most impenetrable computer security regime	
Espionage	Becomes present when stored information holds great value to a threat actor.	Would have to take place when information is electronically available.	Spyware can be installed in the Piql IT system, and thus compromise the confidentiality of the stored information.	Follow the guidelines set forth by Norwegian National Security to ensure the most impenetrable computer security regime	Piql is following the guidelines on computer security set forth by Norwegian National Security. Thus the risk of someone hacking into our systems to perform espionage is reduced to almost non-existing.

Threat/hazard		Details	Consequence	Recommendations by FFI	Comments by Piql
Computer security	Security software	Constant evolving software solutions in a 500-year perspective.	If security software is not kept state of the art, it may leave the Piql IT system vulnerable.	Follow the guidelines set forth by Norwegian National Security to ensure the most impenetrable computer security regime; all hardware & software to be kept state of the art, update security software continuously, never distribute admin.rights to end-user, activate code-protection against unknown vulnerabilities and harden applications to mention a few. We also recommend to offer clients cryptography to protect their information. Though it compromises the vision of being self-contained, this should be up to the individual client to decide.	Piql will follow guidelines set forth by the Norwegian National Security, and will distribute them to the Piql Partner Network. We will also offer our clients the opportunity of encrypting the data they want stored, even though that compromises the self-contained feature of our Services.
	Hacking the Piql IT system		Can i.e. alter checksums used to verify that the information received is the same as the information sent by the client.		
	Lack of cryptographic protection	Piql does not offer the client to crypt their information as it would compromise the feature of being self-contained.	Clients with confidential information may disregard Piql as an option for data storage.		
Inside threat	Piql employee	Can act on their own violation or on behalf on someone else	Can steal original files, damage the piqlFilm physically or remove the piqlFilm altogether	Perform regular security clearance, check of criminal records and credit check of employees. Limit number of people with access. Always work in pairs.	We perform extended background checks of all employees. No employee can access the entire Service Journey. For a file to be retrieved, it will have to be officially requested by the Client. A Piql employee can not retrieve a file on his/her own initiative.
Loss of Ideal Storage Conditions	Loss of utilities	I.e. loss of energy supply which in turn can lead to ventilation system stops working	Higher temperature and humidity than recommended can cause the film to warp, and also blemishes and fungi growing on the film. Lower temperature than recommended can cause the piqlFilm and piqlBox to become more brittle.	Back-up generators, and energy supply from two different sources, i.e. diesel and electricity	The piqlFilm and piqlBox is very robust. Thus the tolerance to fluctuations in temperature and humidity is high. Back-up energy supply, is a part of the requirements for storage facility that we distribute to all Piql Partners.
	Damages to infrastructure of building	Can allow outside air to flow into the storage facility			
"Out in the open"	When the piqlFilm is out if the piqlBox		More vulnerable to physical damage, harmful light and injurious temperatures	Recommend further testing to improve piqlBox to withstand 'rough' physical handling.	Our routines ensures that the time the piqlFilm is out of the piqlBox is minimal, and when this happens, it is under full control of our security routines.
	When the piqlFilm is outside a Piql-controlled environment all together		More vulnerable towards physical theft	Change route of transportation from day to day, or have the production facility and the storage facility at the same location.	We recommend that the production site and the storage facility is under the same roof. If transportation is needed, a background check of driver will be performed and the driving routes will be alternated to reduce predictability.

Piql AS

Grønland 56,
3045 Drammen
NORWAY

www.piql.com