Project Title	Wide – Impact cyber Security Risk framework
Project Acronym	WISER
Grant Agreement No	653321
Instrument	Innovation Action
Thematic Priority	Cybersecurity, Privacy & Trust, Risk Management, Assurance Models
Start Date of Project	01.06.2015
Duration of Project	30 Months
Project Website	www.cyberwiser.eu

<D6.1 - BEST PRACTICES & EARLY ASSESSMENT PILOTS, PRELIMINARY VERSION >

Work Package	WP 6, Pilots
Lead Author (Org)	Atle Refsdal (SINTEF)
Contributing Author(s) (Org)	Antonio Álvarez (ATOS), Romina Colciago (AON), Ales Cernivec (XLAB), Roberto Mannella (Rexel), Dawid Aleksander Machnicki (ATOS), Gencer Erdogan (SINTEF)
Due Date	31.08.2015
Date	05.09.2015
Version	1.0

Dissemination Level

x	PU: Public
	PP: Restricted to other programme participants (including the Commission)
	RE: Restricted to a group specified by the consortium (including the Commission)
	CO: Confidential, only for members of the consortium (including the Commission)

Versioning and contribution history

Version	Date	Author	Notes
0.0	26.05.2015	Atle Refsdal (SINTEF)	Initial draft of structure
0.1	10.07.2015	Antonio Álvarez (ATOS)	Information from Portic Barcelona
0.2	15.07.2015	Antonio Álvarez (ATOS)	Information from Tunstall Ibérica
0.3	30.07.2015	Romina Colciago (AON)	Main international cybersecurity frameworks and standards; Most popular vulnerability assessment tools
0.4	04.08.2015	Atle Refsdal (SINTEF)	Introduction, restructuring of state of practice, appendix for the questionnaire
0.5	07.08.2015	Atle Refsdal (SINTEF)	Method for information gathering (EAPs)
0.6	10.08.2015	Ales Cernivec (XLAB)	State of practice contributions
0.7	11.08.2015	Atle Refsdal (SINTEF)	Information from OTG
0.8	12.08.2015	Ales Cernivec (XLAB)	Information from Koofr
0.9	14.08.2015	Roberto Mannella (Rexel)	Information from Winmedical
0.10	17.08.2015	Dawid Aleksander Machnicki (ATOS)	Best practice: security testing, and vulnerability and threat monitoring
0.11	21.08.2015	Gencer Erdogan (SINTEF)	Best practice: Standards and methods for risk assessment
0.12	27.08.2015	Ales Cernivec (XLAB)	Information from 100 Percent IT
0.13	27.08.2015	Gencer Erdogan (SINTEF)	Best practice: Standards and methods for risk assessment, security testing, and vulnerability and threat monitoring
0.14	28.08.2015	Gencer Erdogan (SINTEF)	Method for information gathering: state of practice

0.15	31.08.2015	Atle Refsdal, Gencer Erdogan (SINTEF)	Information from Mare Beach Wear and FMI,executive summary, common needs, conclusions
0.16	03.09.2015	Atle Refsdal, Gencer Erdogan (SINTEF)	Corrections and modifications after internal review
1.0	05.09.2015	Antonio Álvarez (ATOS)	Version for submission to the EC

Disclaimer

Table of Contents

List of Figures

Executive Summary

This report serves two purposes. First, it describes the business processes, cybersecurity needs and current practice of the associate partners for which the early assessment pilots (EAPs) are conducted, thereby creating a shared initial understanding of these organizations among the consortium members. The EAPs serve an important function in the WISER project, as they provide a basis for understanding strengths and weaknesses of cybersecurity and risk approaches currently in use, identifying needs and requirements, as well as for testing the tools and methods of the WISER framework.

Second, the report provides an overview over standards, methods and tools for security and risk management, security testing, vulnerability and threat monitoring. Here we do not limit ourselves to those approaches that are actually adopted by the associate partners, but also include others that are available and relevant. In order to reflect the current best practice we have aimed to include standards, methods and tools that are considered to represent the state of art as well as being well established and widely used, or at least mature enough to be applied in a realistic industrial context. With respect to standards and methods we have focused in particular on those offered by ISO and NIST, as these seem to have a particularly strong position. The best practice overview provides valuable input for developing the WISER framework, as it describes a number of ideas, approaches and results that can be exploited and built upon to further advance the practice, as well as serving as a benchmark for assessing the contributions offered by the framework. With respect to tools we focus on leading open source and commercial tools for security testing as well as threat and vulnerability monitoring.

This report is a preliminary version written at an early stage of the project. A final version is planned at the end of the first year, at which point we will of course have obtained a deeper understanding of the associate partner organizations, their processes, systems and cybersecurity needs. Roughly speaking, the EAP descriptions provided here represent much of the same information that would typically be collected during the context establishment phase of a risk assessment process along the lines of ISO 31000. To obtain this information from the associate partners we have followed a simple method consisting of four steps: 1) Identify expected content and common section structure for the EAP descriptions; 2) Develop questionnaire to support collection of the information; 3) Collect and document information from each EAP; 4) Identify common features of the EAPs.

The associate partners represent a highly diverse group of businesses and domains, including biomedicine and biomedical research, health care, transportation, bioinformatics, ICT services, fashion, and oil & gas. Even so, there are a number of concerns that are shared by more or less all of them. They all rely on interconnected ICT infrastructure for their critical business processes. Loss or disruption of this infrastructure could therefore prevent them from running these processes and lead to significant economic loss. Many of the associate partners also store or handle sensitive data in their ICT infrastructure, for example relating to patient health or business information that could be exploited by competitors or criminals. The reputation of several of the partners among their clients and society in general depend to a large degree on their ability to protect themselves from cyber attacks. Incidents leading to service disruption or confidentiality breaches could potentially have severe impact on the trust of clients and customers.

One important finding from the set of EAP descriptions of particular importance for WISER is that few of the associate partners have large resources available specifically for cybersecurity and risk management. In many cases, a single individual is responsible for this in addition to other daily obligation, while in other cases there is no dedicated person or group who is responsible. *This shows that it is vital that WISER offers the possibility to adopt and configure the WISER framework in a lightweight manner that does not require large resources and highly specialized skills.*

1 Introduction

1.1 Purpose and Scope

The purpose of this document is twofold. First, we describe the business processes, cybersecurity needs and current practice of the associate partners for which the early assessment pilots (EAPs) are conducted. This helps to create a shared initial understanding of the EAPs between the members of the consortium. The EAPs represent a wide variety of businesses and domains, ranging from sale of beachwear to oil & gas. A thorough understanding of the systems and processes of the associate partners, their current approach to cybersecurity as well as their cybersecurity needs is essential for the WISER consortium when developing the WISER framework, as an important objective for the EAPs is to help obtaining requirements for the framework and ensuring its relevance in practical settings. In particular, although the associate partners appear very different, their needs and concerns with respect to cybersecurity are not necessarily that disparate. *Any innovations that address common needs are of course more likely to be of general value also outside the consortium and associated partners.*

Second, we provide an overview over standards, methods and tools for security and risk management, security testing, vulnerability and threat detection and monitoring that are currently available and considered to represent best practice. This also serves as valuable input for developing the WISER framework, as it offers a number of elements that can be exploited and built on to further advance the practice.

1.2 Relationship to other project outcomes

As indicated by its title, this document (i.e. D6.1) is a preliminary version written at an early stage (month 3) of the project. Roughly speaking, the descriptions of the EAPs given here represent much of the same information that would typically be collected during the context establishment phase of a risk assessment process conducted along the lines of ISO 31000. Here, a central goal is to establish an understanding of the target of analysis, including the goals of the organization in question, as well as the systems and processes to be analysed. The findings here has helped established the set of requirements that are documented in D2.1 "Requirements", which again form the base for D2.2 "Framework design, initial version" and D2.3 "Framework design, final version". The requirements from D2.1 will be further evaluated through workshops organized by task 6.1 in the context of the EAPs. D6.1 also obviously forms the basis for the final version, i.e. D6.2 "Best Practices & Early Assessment Pilots, Final Version", which is due in month 12 and will provide reports on the results from each of the EAPs, with indications for the technical and business requirements of the WISER methodology and platform. At that point a much deeper understanding of the EAPs will of course have emerged through further interaction with the associate partners and analysis of their systems and processes.

1.3 Structure of the document

The rest of this document is structured as follows. In Section 2 we explain the method used for gathering the information presented. Section 3 presents the business processes, cybersecurity needs and current practice of the associate partners for which the EAPs are conducted, while Section 4 discusses their common needs and challenges. Then we move on to describing the state of practice in three sections. Section 5 addresses standards and methods for risk management, Section 6 addresses security testing, while Section 7 presents vulnerability and threat monitoring. We then conclude in Section 8.

2 Method for information gathering

2.1 EAP descriptions

Figure 1 gives an overview of the method that was used to arrive at the EAP descriptions documented in Section 3. In the following we further explain the steps involved.

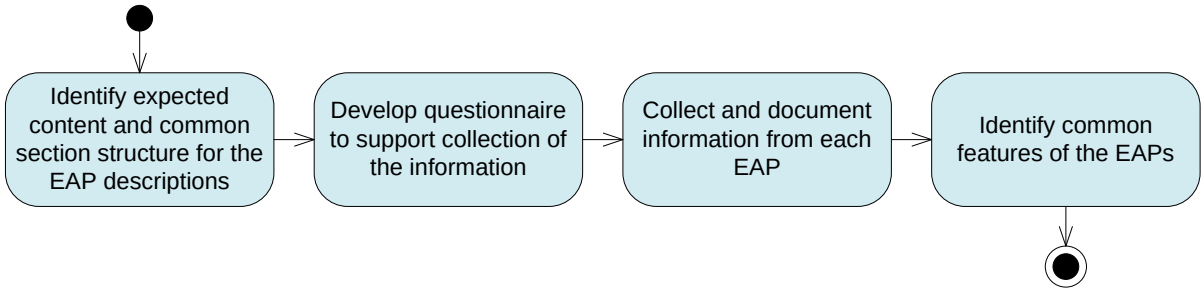

Figure 1: Method for EAP descriptions

The first step was to identify the expected content from the EAPs. This was done by establishing common headings to define the structure for presenting each EAP description. For each heading a short guideline text was provided to indicate the expected content. The result is reflected in the structure of the descriptions presented in Section 3. We also identified which members of the consortium would be responsible for collecting the information from each associate partner, taking into account competence as well as geography and relations to the associate partners. To further support the collection of the information, the next step consisted of developing an open questionnaire to be used in communications with the associate partners for which the EAPs are conducted. After a first draft had been created, the questionnaire was modified as a result of discussions and e-mail interactions within the consortium. Appendix I shows the final version.

The third step was to collect and document the information. This was done through physical meetings and/or telephone conferences with the associate partners depending on their availability, preferences and practical considerations, as well as e-mail interactions. The responsible consortium members that had earlier been assigned to the associate partners took care of arranging and leading the meetings and documenting the results.

Finally, after the descriptions of the EAPs had been obtained, the fourth step involved identifying commonalities between them. This was considered with respect to business processes, system types, ICT infrastructure, cybersecurity concerns, needs and current practice. The results are documented in Section 4.

2.2 State of the practice

As illustrated in Figure 2, we identified current best practice relevant for WISER following three main steps. In the following we explain how each step was carried out.

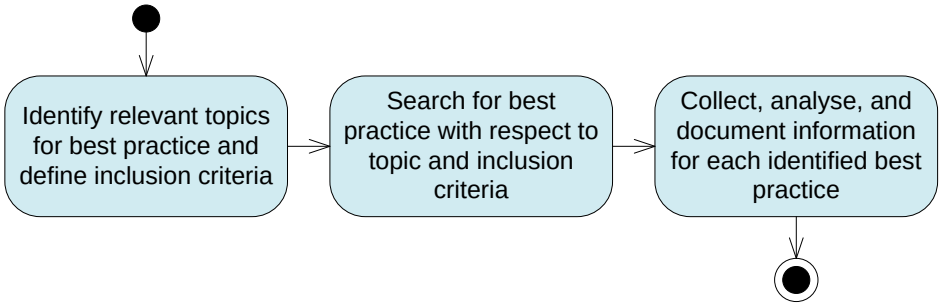

Figure 2: Method for state of the practice

In the first step we identified relevant topics to be covered by the best practice, as well as an overall inclusion criterion characterizing what may be regarded as best practice. We identified three main topics to be covered by the state of the practice: standards and methods for risk assessment, security testing tools, and vulnerability and threat monitoring tools. These topics are covered in Sections 5, 6, and 7, respectively. With respect to inclusion criteria, in order to reflect the best practice we aimed to include standards, methods and tools that

- are considered to represent the current state of the art, and
- are well established and widely used, or at least mature enough to be applied in a realistic industrial context.

Similar to the method for EAP descriptions, we also identified which members of the consortium would be responsible for contributing to the aforementioned topics in order to exploit competence and areas of expertise.

In the second step we searched for standards, methods and tools related to the above mentioned topics with respect to the inclusion criterion. While searching for standards and methods, we mainly based ourselves on standards published by the International Organization of Standardization (ISO) and the National Institute of Standards and Technology (NIST), as well as leading risk assessment methods in the industry and government. Moreover, to obtain a holistic picture we first studied the well established standards and methods and, based on that, identified other related standards and methods in a top-down approach, as described in Section 5. With respect to tools, we mainly focused on commercial and free tools widely used for the purpose of security testing and monitoring. Notice that the descriptions of the tools are to a large degree based on the information made available by the tool providers, as we did not have the opportunity to try out the tools.

In the third and final step we analysed the collected information and documented the state of practice as shown in Sections 5, 6, and 7.

3 Business processes, cybersecurity needs and current practice of the associate partners

In this section we present each of the associate partners for which the Early Assessment Pilots are conducted. Each presentation follows the same structure. First we present the organization and business goals, then the critical business process(es), and finally the cybersecurity needs and current practice of the organization.

3.1 Portic Barcelona

3.1.1 Organization and business goals

Portic Barcelona is a company whose mission is to organize the necessary document exchange, performed in a specific set of defined workflows, happening during the processes of goods receipts and issues at Barcelona port. Portic aims at improving the competitiveness of the companies belonging to the logistic community of Barcelona port. To do so, Portic is in charge of providing the needed ICT infrastructure to support this process, this is, a technological platform that eases the interaction among them. Portic provides a *Port Community System* (PCS). A PCS is defined as *an electronic platform that connects the multiple systems operated by a variety of organizations that make up a seaport or airport community. It is shared in the sense that it is set up, organized and used by firms in the same sector – in this case, a port community* [6].

Portic technology enables the real-time tracking of any container, both its physical location and its documental management, by means of the traceability of all its events. It is especially important the correct management of those containers transporting dangerous goods. Besides, Portic offers a datawarehouse which allows the aggregation and processing of relevant statistics concerning the activity at the port.

Portic Barcelona is a company which does not have any binding to any of its clients, being neutral in such sense. It is a company whose shareholders represent the main stakeholders involved in the daily operation of the port (except for the final users, who are not shareholders anymore) [1].

22 people compose the staff of Portic Barcelona. Reporting to the CEO, there are five departments that involve people having different professional profiles: Financial, trading, technical, consulting, client care and international business development.

Portic aims at providing its clients with some technological means to benefit the performance of their daily tasks at the port:

- Reduction of the time to search and exchange information, also reducing the mistakes in documentation.
- Reduction of operational costs such as phone calls, delivery men or people devoted to document management.
- Increase on efficiency when managing goods by means of real-time planning and programming of the daily work at the port.
- Proactive troubleshooting.
- Legal certainty, since Portic provides a legal framework among the different parties. Commercial security by ensuring that all the people involved in the daily activity are duly authorized and security as for information confidentiality by preventing non-authorized accesses.

Portic intends to boost the activity at Barcelona port by progressively empowering the ICT infrastructures provided to its clients. The main KPI to measure the success is the number of messages managed every year. In this sense, the operation capacity of the company has experienced an exponential growth.

3.1.2 Critical business process

As presented in the previous section, Portic plays the role of a broker exchanging messages in the context of the different workflows performing the logistics of Barcelona port. These messages mostly have the format of XML files. These files contain information about the movement of the containers in the port, what they contain and the different agents (both public and private) involved in the management of each container.

These workflows can be represented by means of sequence diagrams [3] where the different actors participating in the process are unequivocally identified and where the different kind of messages that can be exchanged also belong to a closed set [2][4]. Figure 3 shows a sequence diagram where it can be seen that the actors are represented in the columns and the documents/messages exchanged among the actors are represented by arrows.

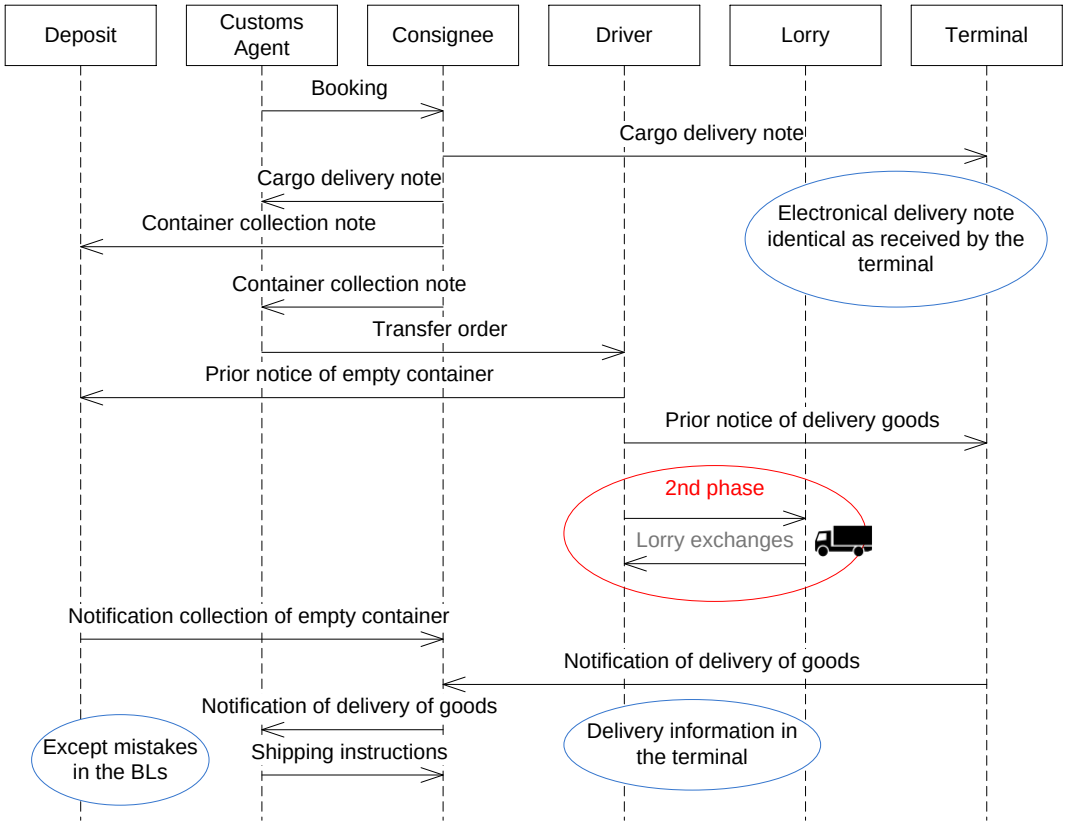

Figure 3: Portic Barcelona. Example of document circuit [3]

The most important asset is the Data Center, which contains the implementation of all these workflows and all the information related to them. This is logistic and transport information, but also commercial information, since it is possible to find out information related to commercial partnerships between different companies operating at the port by means of a thorough analysis. Then, this information becomes valuable and something that needs to be properly protected by putting in place the adequate means. This Data Center processed around 18 million messages in 2014. The Data Center is expected to help to optimize and speed up the management of containers and goods within the port. Not only the information contained is very valuable, this asset has to offer very high availability during the working day. It manages the reception and the shipment of goods and all the needed documental procedure to carry out in compliance with the regulation and in a secure manner. The unavailability of the Data Center might entail a serious setback in such a sensitive and complex working environment with high control requirements.

The operation at Barcelona port is based on identifiers associated to each container movement. Each identifier is linked to all the agents that will take part in the whole workflow. There was the need to establish a trade-off between the needed security and the agility to operate. This means that some steps of the workflow are not associated a physical person by default. This opens the possibility for intruders to sneak in the process if they are able to get hold of the credentials belonging to one of the platform users and access the information related to the management of containers. This process is used by criminals to steal valuable goods from the containers or introducing drugs. They would only need the information about the container and the following steps in the accomplishment of its delivery to carry out their malicious purposes.

Another sensitive data is the reservation code when a specific resource is needed. This reservation code is exchanged among different actors and circulates in the mails that are exchanged, where it remains stored, what means that is stored in servers beyond the ones controlled by Portic.

The need for this trade-off makes the process weak at some steps, and these are the vulnerabilities the criminals want to exploit in order to commit their crimes. They will try to get the control of the system in order to use the port to fulfil their goals.

Portic provides the communication network needed for the exchange of documentation and the management of containers at the port. The client starts the process by generating the message and transmitting it by means of HTTP or FTP. The system works like a mailbox and the client can retrieve the messages related to all the process involving him. If the client cannot generate the message with his own means, he can also use Portic application offering this feature.

The architecture consists of

- An application server which acts as a message broker.
- A communications server.
- A mailbox server where messages are processed to be delivered to their addressees.
- An Oracle database.

The applications are implemented following a three-layer-architecture. The general process a message undergoes is the following:

1. Message composition
2. Authentication and authorization of the user
3. Validation of the message content
4. Database updating
5. Delivery of the message to its addressee.

The management of the Data Center is outsourced to an external company. The information is replicated somewhere else by means of a backup process. However, the Data Center itself is not replicated, which means that, were it not available, there would be no service until its recovery. The communication architecture supporting the Data Center is properly duplicated.

There is also in place a monitoring system, watching over the values of a certain set of metrics and raising alarms if any of those metrics crosses a predefined threshold.

Regarding the degree of dependency the critical business processes may have on the correct functioning of the ICT infrastructure, Portic Barcelona acknowledges that to a great extent they have to rely on such infrastructure, but also a non-negligible part depends on themselves and their good/bad practices and policies as for security. Around 400 companies make use of the system on a daily basis. Different user having different roles are allowed to access to the system. In general, the IT knowledge of these users is not high. They do not have good acquired security habits. They do not usually take care of storing their credentials in a safe place. In general, they are not aware of how important their credentials are and the likely consequences of them falling into the wrong hands.

3.1.3 Cybersecurity needs and current practice

As specified previously, the Data Center, and the information it contains, is the most important and sensitive asset to protect. Getting hold of the control of this information, along with some knowledge on logistics, may allow criminals to carry out their actions using the port resources. This means theft of goods or smuggling, among other possibilities. Portic Barcelona identifies as main threats the identity theft and the Denial of Service attacks.

The identity theft allows the criminal to access sensitive information about operations taking place at the port. Moreover, this allows him to actively participate in them. As mentioned previously, there are some operations that, for the sake of simplicity and efficiency, do not need to be associated the identity of a physical person. A clear example would be the criminal knowing that a container of his interest needs a truck driver to be transported to its destination. If the criminal has managed to sneak

into the system with the credentials of a user who can access to this information, he may show up with a truck ready to receive that container and “take on” that shipment.

There is also information related to commercial relationships among different stakeholders. This information may be also used to damage companies´ interests with regard to their clients.

Portic concerns focus on the Data Center and its information being adequately protected. This has to be compatible with the flexibility conceded to make processes more agile.

Portic acknowledges difficulties as far as the credentials management is concerned. Users from around 400 companies deal with the system on a daily basis, most of them lacking of IT security culture. For instance, they are unlikely to change the password periodically, neither do they know some basic rules to strengthen passwords. Even the people with the highest responsibility fail to take care of certain aspects of security. A clear example is that of an employee who quits and subsequently joins a competitor company also working at the port. Not few times does the former employer forget to remove his user from the system, which might result in a notable breach.

Denial of Services attacks provoked some crisis periods in the past. These attacks reduce notably the available bandwidth to communicate with the Data Center and use it. If this happens, it is not possible to continue the normal operation at the port and the reception and issuing of goods has to be interrupted until the IT staff solves the problem and the service is available again.

The progressive activity growth at the port entails a meaningful increase in the quantity of messages circulating and the volume of information stored and managed. This also means a higher and higher dependency on the correct operation of the Data Center and the whole related infrastructure, which has become a key asset. The operation based on paper documentation, delivery men or phone calls seems to have been left behind. However, the operation in paper has to be foreseen if it is not possible electronically [5]. Having such a sensitive asset on which the main business processes depend makes necessary to devote specific human resources to security and to watch over the correct functioning of the whole system. That is why it was decided to count on specific people, with the appropriate professional profile, to deal with these issues.

Besides, as mentioned before, a monitoring system has been implemented. This system is in charge of keeping track of the values of a set of metrics and raise alarms should those values cross defined thresholds. These monitoring systems are outsourced to an external provider. Portic is aware of the fact that the user is the weakest part of the chain. They are trying to work out a solution to improve the relation with the clients. This is one of the main goals of the human resources devoted to security. A possible measure would be to force them to periodically change the passwords, but given the profile of the people dealing with the system this could complicate things rather than be helpful.

The cyber risk assessment procedures are still at an early stage. Each two years, the infrastructure undergoes an audit process and the auditors give some recommendations to follow until the next audit. Portic takes seriously this advice and implements carefully the suggested policies and measures. The recent experiences with regard to cyberattacks have had a positive side, since the knowledge on the matter has been improved. For instance, investigating Denial of Service attacks took some time until discovering that this kind of attacks could be detected by analyzing the firewall logs. If the logs reported bandwidth consumption much higher than usual, it was very likely a Denial of Service attack taking place. The Police have also given some insights that can help to discover criminal activity. For instance, if a container is visited more frequently than usual, this could be suspicious. This can be mapped to the system as some kind of rule: if there is a quantity of messages related to a container higher than usual, an alarm could be raised.

Portic, in collaboration with its providers, has made a leap forward as for the definition of response protocols in case a cyberattack takes place. These protocols are already defined and are being implemented step by step following a planning and devoting specific budget items at each step. Apart from the response to this specific kind of attacks, there is a complete manual of responses to several contingencies mainly associated to the unavailability of services [5]. Figure 4 shows some workflows where how to proceed for each contingency is detailed.

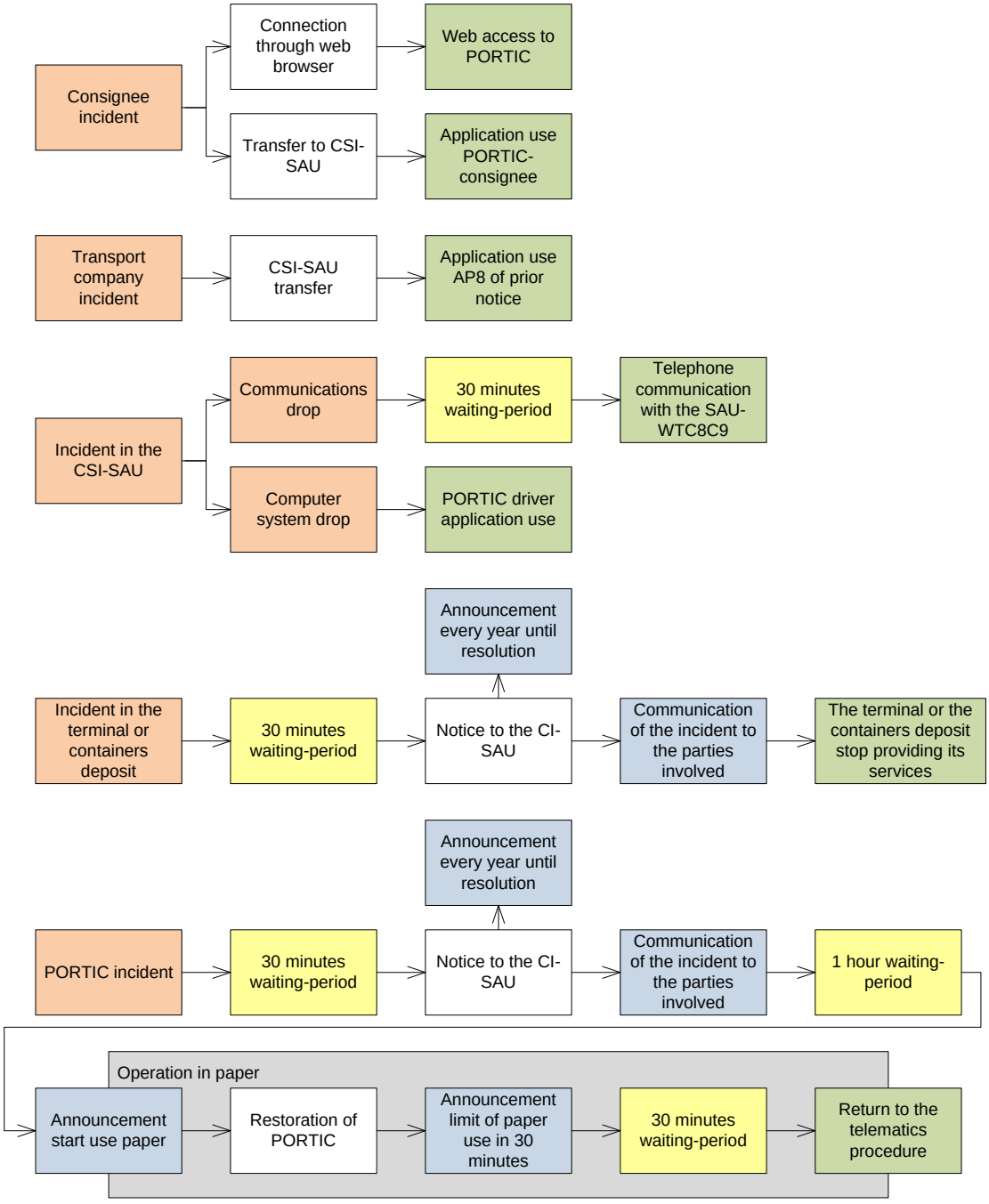

Figure 4: Contingency management workflows [5]

3.2 Tunstall Ibérica SL

3.2.1 Organization and business goals

Tunstall Televida [11] solutions have been designed with the purpose of improving the quality of life, by providing the users the possibility to stay at home, and rely on the fact that they will receive help if needed.

Although technology by itself is not the response, if it is used as a part of a comprehensive service pack it may help to ensure that healthcare and social resources are used efficiently.

Both individual households and environments such as retirement homes can benefit from the extensive portfolio of solutions for remote assistance and monitoring.

This organization leverages technology to offer cutting edge services in the field of healthcare. Tunstall Televida is a part of the group Tunstall Healthcare, worldwide leader in service delivery, software development and manufacturing of remote assistance equipment, remote monitoring and integral communication systems for hospitals and social-health centers, having more than 3,6 million users in 50 countries.

Tunstall Televida is in charge of managing around the 32% of remote assistance users in Spain. This means around 245000 users. They have presence in 10 different cities in Spain (Barcelona, Bilbao, Granada and Murcia among others).

The company counts on the expertise of more than 1300 highly-qualified people, of whom 540 are practitioners in the field of remote assistance. Out of these 540 people, 350 have a university degree related to the social topic (coordinators, remote assistance officers and installers). Tunstall Ibérica provides up to the 60% of the technology used in Spain of remote assistance. Besides, the company also possesses quality and environmental certificates: AENOR 9001 and 158401 for remote assistance and ISO 9001 and 14001 for technology [7], [8], [12], [13].

3.2.2 Critical business process

There are some critical business processes that rely on the appropriate operation of the technology in place.

The process of receiving alarms is quite critical, especially from the point of view of the user´s health. There are several assets involved in the process whose performance becomes crucial, namely:

- The devices installed and configured at user´s home (individual or residence).
    - The technology already deployed at the user´s home must be 100% available and with no faults. A protocol in case of unavailability is established so that the staff can go to the site or connect remotely.
- The communication lines: landlines, datalinks (both wired and wireless – HsxPA, UMTS, GPRS, EDGE – according to the device).
    - A particular case to put special focus on is the one of the communications aimed at the mobilization of resources (emergency telephone number, ambulances, Police, etc.). It is crucial these employees, who carry out interventions at user´s home, to be available and accessible, given the importance of their tasks
- The Management Platform.
- The user care centre.

There is an ICT infrastructure that supports this whole process. There is no outsourcing, Tunstall owns the infrastructure.

There are a couple of main Data Processing Centers, which balance resources and offer reciprocal support to the different systems. Besides, there exist several communication rooms distributed among the different centers.

The infrastructure is properly replicated both internally and externally. The terminals installed in the different residences are communicated by phone with the corporate platforms.

Besides, there are several Call Centers that coordinate the activities, receive and handle the calls and perform the follow-up calls each user needs.

The core network, the applications and the multiple terminal devices are assets whose appropriate operation is crucial for the good health of the business. Furthermore, given the sensitive field in which Tunstall Televida is involved, the health, well-being and even the survival of the customers (in case of severe crisis) highly depend on these assets offering the expected performance.

3.2.3 Cybersecurity needs and current practice

Tunstall Televida considers that the most valuable asset is the data from the users. Tunstall Televida takes seriously their commitment to the confidentiality of people information.

The organization devotes one person part-time to take care of the issues related to cyber security and cyber risks. By default, the cyber-infrastructure undergoes a risk-assessment every year. Nevertheless, if a meaningful change in business processes or a new initiative has a big impact on the infrastructure, or if there are significant changes in the infrastructure, this analysis is anticipated. The used methodology is based on ISO 31000 (an adaptation of the rules for Corporate Risk Management has been implemented, and there is a permanent committee established to follow-up the fulfilment of these rules). Besides, Magerit [9] has been simplified and is also considered for risk assessment.

In order to monitor the cyber infrastructure and detect likely attacks, Tunstall Televida count on a solution which monitors the systems real-time connections, their activity, and the management of the mobile devices.

In case a cyberattack takes place, there is Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRP), for the critical information systems.

3.3 OTG Solutions AS

3.3.1 Organization and business goals

OTG Solutions is a part of Oilfield Technology Group AS (OTG), which is a Norwegian independent group whose core services are Field Operations, Drilling & Well Management, HSE (Health, Safety and Environment) & Offshore Safety Management, Project and Risk Management, Engineering Support and Software Solutions. In the OTG group there are 75 employees, with an annual turnover at approximately 100 mill NOK (11 mill Euro). Oilfield Technology Group AS is divided into three independent companies, as illustrated by Figure 5.

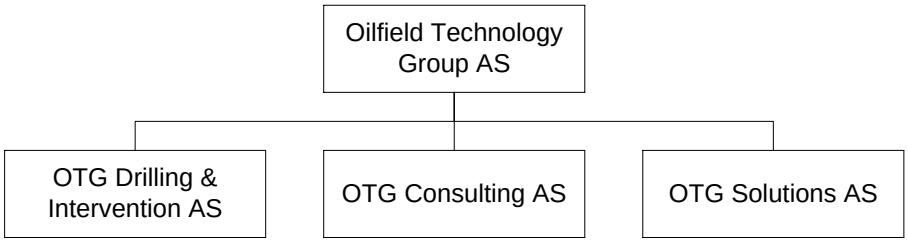

Figure 5 Oilfield Technology Group AS

- OTG Drilling & Interventions AS provides drilling and well related projects and services, skilled and experienced drilling and well supervisors, drilling and completion engineers, safety advisors and HSEQ engineers.
- OTG Consulting AS provides highly qualified and experienced engineers for technical project support and senior engineers in the technical safety/loss prevention disciplines, automation and control systems, fire and gas detection, fire water systems and risk analysis.
- OTG Solutions AS is the R&D and technology development center. The skilled software R&D team has developed many successful software solutions for leading Oil & Gas companies.

OTG Solutions consists of senior programmers and project managers. They develop their software mainly in-house but are also using sub suppliers when needed.

The EAP will be conducted for OTG Solutions AS. OTG Solutions AS is a provider of risk management and operational efficiency software solutions for the global petroleum industry. The main product is the Dynamic Risk Management Center (DRMC). DRMC is a web based risk management database and collaboration system to support management of operational safety risk on petroleum rigs. It can be used, for example to support decision makers when determining whether to allow potentially hazardous operations within a given time frame. DRMC has been developed based on OTG's broad, project-based and hands on understanding of the oil and gas industry. From DRMC they have developed a broad range of products for in-house use and for clients. DRMC can be used as a stand-alone solution, or be integrated with their clients' current IT infrastructure.

The main business goal is to assist OTG's clients in reducing risk, avoiding major accidents and improving operational efficiency.

In DRMC the focus is on geographical visualization of risk factors and user friendliness to enable users to have a bird's eye view of the present operational risk picture in projects and operations. Risk factors can be shown in their relevant location on a map of the rig, using a simple colour scale to illustrate risk level. The systems require no local installation, and can be accessed on all platforms (PC, tablets and smart phones).

3.3.2 Critical business process

As DRMC is the main product of OTG Solutions and cybersecurity is a fundamental prerequisite for its successful application, the operation of DRMC is the critical business process on which the EAP will focus. The DRMC solution is in general delivered as software as a service (SaaS) solution, but is also customized and configured to special clients/project needs. Figure 6 shows an overview of the main use cases of DRMC operation as a UML use case diagram (the development of the DRMC solution is not included).

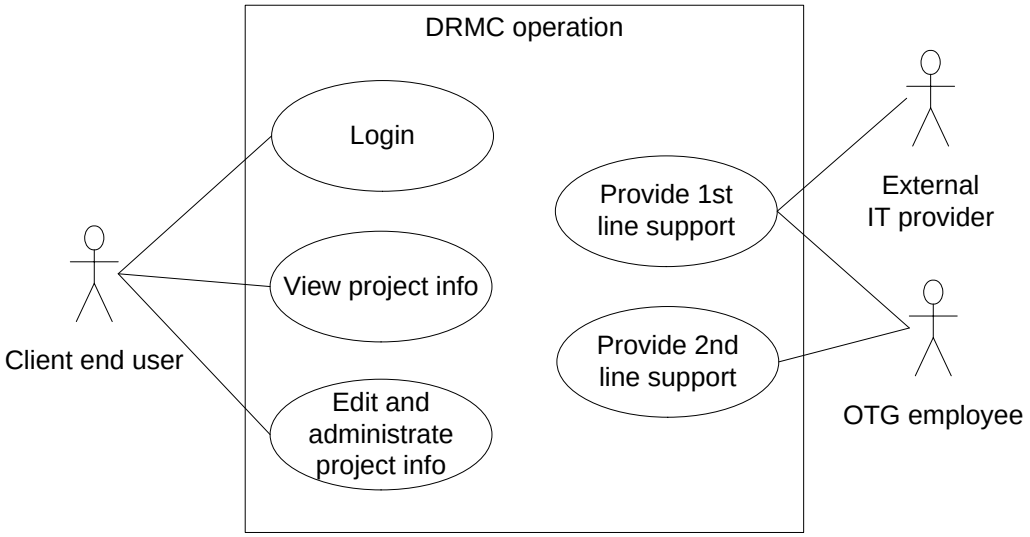

Figure 6 Use cases of DRMC operation

Access to the different products/modules is controlled by a unique user ID and password. The users can access the system via a web browser when in a range of a network/Wi-Fi. Users with access to a DRMC product can view, edit or administrate in their project depending on the level of access, giving all other users an instantly updated overview of all risk factors and changes. The system will automatically track all changes by who, when, what, to give an individual change management and

history file. First and second line service is provided by OTG internally, but for 24/7 projects first line support will be will be handled by an external IT provider.

A high-level overview of the ICT infrastructure of DRMC is shown in Figure 7.

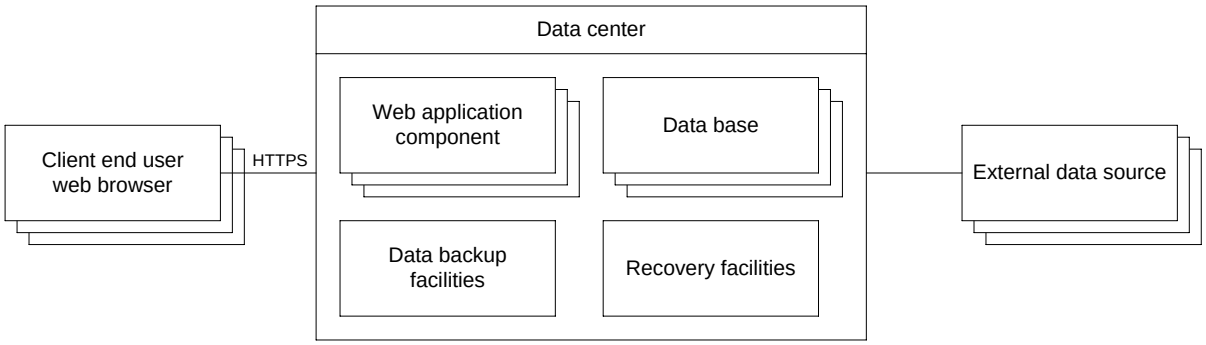

Figure 7 DRMC infrastructure

At the core of the infrastructure lies the data center, which is located at Cegal (http://www.cegal.as/home), which is the infrastructure partner of OTG Solutions. Cegal provides the server system, which is running the databases and the web application components of DRMC. The service also includes data backup facilities and recovery services.

Each client end user interacts with the data center using a web browser accessing the data center through an https connection, as illustrated by the left-hand rectangle of . This ensures that local installation on the client side is not needed.

As illustrated by the right-hand rectangles, the data center is connected to a number of external data sources to collect data that will aid the decision processes of the end user. The decisions in question are typically related to safety risk issues. Examples include whether to allow work that involves welding ("hot work"), outdoor work or work above sea on an offshore petroleum installation in the next 24 hours. These kinds of decisions depend on what other activities will take place, the weather forecast, the presence of supply boats, and so on. This type of information is collected from the external data sources. Information from such sources is typically either fetched through standardized APIs, where available, or scraped from their web pages through specialized processes. The following data are fetched from external sources:

- Rules and regulations for processes, equipment, building codes, etc from a range of sources: Petroleum Safety Authority Norway (http://www.ptil.no/), Norwegian Maritime Authority (https://www.sjofartsdir.no/), the Norwegian Oil and Gas Association (https://www.norskoljeoggass.no/en/), and others.
- AIS (Automatic Identification System) positioning data for supply ships and movable rigs, from MarineTraffic (http://www.marinetraffic.com/en/).
- Weather information for the North Sea and bordering coastlines, from public Norwegian weather service Yr (http://www.yr.no/).
- Heliport schedules for traffic to and from the North Sea rigs, from heliport.no (http://www.heliport.no/) and Avinor (https://avinor.no/).
- Supply base information, from various public services.
- Most of the above mentioned data sources are visualized in various contexts in a 2D map service, using Leaflet maps technology and tile data from the OpenStreetmap public project.

Other parts of the system, such as the authentication service and security breach detection software, are insourced, using commonly known and widely available software parts such as OAuth and Tripwire.

Regarding the criticality of the business processes that depend on the DRMC infrastructure, it should be noted that although DRMC does not control any technical system on a facility, it has an important function as a decision support system that handles and visualizes data, thereby giving the users a better overview of risk factors when planning and operating the facility. The DRMC system will also look for conflicts in the data sets and give warnings to the users if any known critical situation is identified. If a loss or damage to the ICT infrastructure supporting DRMC occurs so that DRMC fails to function as intended, it could lead to an end user taking wrong decisions or not being able to identify a critical situation that is under development. The following illustrate the criticality:

- Without access to the correct risk information it is not possible to make good decisions. This can result in costly delays or, in the worst case, lead to a major accident on an installation. The latter may occur if, for example, hot work is planned in a process area without being aware that a fire detection system has been taken out of service in a nearby area.
- If the system is showing incorrect or corrupted data, it will lead to misinterpretation of the current risk level and potentially result in wrong decisions. For example, showing a critical deviation in the wrong work area could lead to delays of work in the area shown and increase risk level when doing activities in the correct area.
- The system handles sensitive operational and project data. In some cases information from DRMC can be very critical and can be misused by someone with wrong intentions. For example, if a critical risk factor identified in DRMC will cause a major delay in a development project, then this can be stock sensitive information for the clients/customers of OTG.
- Cyber-incidents causing downtime in the 24/7 products/modules offered by OTG will have major impact on their business. This will definitely damage reputation and sales for the OTG software products.

3.3.3 Cybersecurity needs and current practice

The DRMC server (running in the Data center) and the client data are the most important assets for OTG Solutions that could potentially be harmed by a cyber-incident. More specifically, the focus is on the integrity, availability and confidentiality of the client data, as well as the integrity and availability of the DRMC server itself. The cybersecurity needs of OTG Solutions therefore concern the protection of these assets. Their current cybersecurity practice can be summarized as follows:

- A dedicated and competent senior programmer is responsible for cyber-risk at OTG Solutions. The responsible resource has 20 years of experience in a wide variety of areas of competence related to server administration and security issues.
- Risk assessment of the cyber-infrastructure that supports the critical business process described above is conducted approximately quarterly, but is done on an ad-hoc basis and varies with demand. Security audits and evaluations are typically done when new partners or customers are introduced.
- For risk assessment OTG Solutions base their activities on ISO 27001 as well as checklists developed by one of the leading oil companies. With some exceptions they claim compliance with ISO 27001, but certification has not taken place.
- Commonly used Tripwire intrusion detection systems are in use for automated real-time monitoring of the cyber-infrastructure.
- A recovery plan is in place in case of damage as a consequence of cyber-attacks. Briefly speaking, the plan is as follows:

- On detection (or suspicion) of serious intrusion of the system, or any other security breach, the plan for recovery is to take down the affected server and re-instate a fresh set up from data backups. The system has been designed with quick re-installation from scratch in mind, and all developers have a personal full system installation to secure the viability of the recovery plan.
- The compromised system which was taken offline will then get a full post hoc analysis/autopsy, in a sandboxed, fully secured environment, to find the cause of the breach.

3.4 Koofr d.o.o.

3.4.1 Organization and business goals

Koofr was built to address and effectively solve the problems of concern about the physical location and transparency of security of the data hosted by the cloud providers. Koofr is a cloud storage provider and provides a hybrid cloud storage alternative. Using Koofr, users are able to manage and share their data easily, regardless of the underlying storage system, and by using a trusted cloud provider. Koofr provides the technology that allows users to manage and share local, remote and cloud stored files with a single, easy to use interface – even users themselves can provide the trusted service. There are several ways that Koofr differs from existing cloud storage solutions. Not only that users can use mobile applications on all mobile platforms and web interface, even applications and users can connect to Koofr storage via existing secured API calls from advanced client services. All provided applications talk with Koofr's public API. Koofr also provides combination of custom storage systems (e.g. connection to existing user's storage on Dropbox accounts, existing Google's Drive storage systems or home computer's storage). Users can connect their own local storage (on their computers) to Koofr. This is made possible with a custom protocol tunneled via an HTTP WebSockets connection. Clients maintain a persistent connection through which the Koofr service sends file operation requests, and fetches file data and metadata. If needed, users are allowed to implement their own clients and integrate data stored on Koofr into their workflows. Koofr also provides a WebDAV implementation for easier integration with existing applications.

Koofr is an SME, employs 5 people. It currently has paying customers from all over the world. Since Koofr provides technology as a white label solution, it can easily be integrated with existing cloud services. Koofr provides white-label services to ISPs mainly from EU.

3.4.2 Critical business process

Critical business processes consist of interaction between critical services providing:

- Maintaining deployment of white-label Koofr services
- User accounts and storing credentials securely on back-end storage,
- Payment process of Koofr users
- Databases holding user-related data
- Development process: consisting of storing sources and releases of the service, deployment infrastructure
- Monitoring process of Koofr services based on Icinga (open source solutions)

Koofr supports multiple kinds of storage backends: provider hosted storage, public cloud storage, and native client storage. Communication between Koofr services and each of these backends on the client must be secured.

Koofr platform is installed on a per-customer basis. A customer provides remote access (SSH) to servers with minimal OS install and Koofr takes care of provisioning and deploying, and provide assistance for configuring the network.

3.4.3 Cybersecurity needs and current practice

Koofr is built modularly. The platform consists of (logical) application and database nodes. Individual logical nodes can be deployed on a VM or a physical server, running the GNU/Linux operating system. Most valuable services that are susceptible to cyberattacks are:

- Main front-end node with HAproxy services (risk: connecting a malevolent application node in the cluster)
- Web component with SOAP and REST interface to the platform, Koofr's public API. It takes care of authentication of API clients and displays static pages.
- API component that handles Authentication, Authorization and Accounting (AAA), user management, team management, notification services, sharing, comments. Authentication and identity management can also be provided through a custom integration module, tailor-made for the client's proprietary AAA infrastructure. Risk: malvolent authorization node. It is possible to integrate with external SSO systems providing e.g. SAML responses. The responses need to be digitally signed and submited over encrypted communication channels
- Database node is critical infrastructur- metadata database representing user's filesystem

Risk assessment of the cyber-infrastructure supporting the business process is conducted on an ad-hoc basis and varies with demand and development of the product. Additionally, security audits and evaluations are done on-demand by new partners or new customers. A recovery plan in case of intrusion or compromised system is that the compromised part of the solution can be easily replaced as soon the detection of the intrusion is made. Therefore, the recovery process is already handled by architectural design of the system (built-in recovery plan). The system is provided by the monitoring infrastructure already. It is based on monitoring services for log files (log checker) and network monitoring (module for monitoring network traffic on the infrastructural node of the system). A recovery plan in case of detected infrastructural defect is also handled and thought of in the architecture of the system: built-in recovery plan (in line with: "forget the node and create a new one").

3.5 Winmedical

3.5.1 Organization and business goals

Winmedical was founded in Pisa, Italy in March 2009 as a spin-off of the "Scuola Superiore di Studi e Perfezionamento Sant'Anna and began its business operations in 2010. Today, Winmedical employs 18 people with a turnover of more than 1M€ annually. Its operations are focused in two main market segments:

- Sales of Wireless IIAC CE marked multi-parameter monitoring devices
- Remote patient monitoring services

The two aforementioned market segments are valued annually at $1.9B USD and $20-$30B USD respectively. From those markets segments, the main business goals for Winmedical are as follows:

- Reduce health care costs which are growing annually

- Improve the quality of life for patients through continuous monitoring for signs of degradation as an early warning to seek medical treatment
- Decrease the average number of days that patients spend in the Intensive Care Unit (ICU)
- Decrease patient readmission rates

In order to achieve it main business goals, Winmedical has three product offerings in the market: WINPACK, WIN@HOSPITAL and WIN@HOME.

3.5.2 Critical business process

Winmedical is both ISO13485 and ISO9001 certified and as such, it has many processes that are critical to its business. Primarily, the critical processes are in R&D as Winmedical invests approximately 20% of its annual turnover in R&D activities.

In conjunction with its R&D activities, Sales and Customer Service are the other main aspects of Winmedical's business. As they are relatively new to the market, Winmedical works diligently to interact with its customers to establish relationships and credibility for its products and services. They closely monitor their installs bases' performance, quality and customer experience and are always on the lookout for potential new revenue streams.

From an Information and Communications Technology (ICT) both the R&D and Sales and Customer Service activities within Winmedical are heavily supported by ICT related infrastructure.

In the R&D realm, Quality Assurance (QA) and Total Quality Assurance (TQA) activities are essential to ensuring that their products and services operate together flawlessly. This is achieved by end-to-end testing conducted within the organization's laboratories and these activities rely heavily on ICT infrastructure.

The Sales and Customer Service activities leverage ICT infrastructure on many levels that can be outlined by three different supporting roles in the sales engagement:

- Sales
    - During the sales process, demonstration units are provided and showcased and the sales staff utilize a combination of laptops and iPads for this activity
- Product Specialist
    - During the demonstration, the Product Specialist details the capabilities of the devices, probes and sensors that comprise Winmedical's product offerings
- Technical Specialist
    - Once products and services have been procured for a customer, the Technical Specialist is a liaison between the client and Winmedical IT support. Activities such as coverage area testing is conducted with laptops and devices to ensure that stable and reliable service is achieved

3.5.3 Cybersecurity needs and current practice

In terms of cybersecurity at Winmedical, there are two major assets that would be considered most important to its operation.

The primary asset that Winmedical needs to protect is patient data. Virtually all countries that Winmedical operates in have legislation regarding the protection of patient medical data. For example in Italy, hospitals and healthcare providers are not permitted to send patient data into the

cloud if their servers are on premise. Regulations around the exchange and protection of patient data must always be respected.

A second potential area of risk for Winmedical exists around the servers in the organization that are used to connect to clients' systems for technical purposes as well as storing its documentation and clients' and suppliers' data. Data breaches on such systems could have a significant, negative business impact on Winmedical.

Presently, Winmedical does have a dedicated resource responsible for cyber risk and cybersecurity and risk assessments are conducted on an annual basis as part of the internal audit for its ISO13485 certification. They also have recovery plans in place in the event a major security incident occurs.

However, Winmedical does not follow a standardized approach for risk management or assessment specifically around cybersecurity (this does exist for their medical devices as part of their ISO13845 certification). They also do not have any real-time detection or prevention of potential cyberattacks that may occur.

3.6 100 Percent IT

3.6.1 Organization and business goals

100 Percent IT is a UK based Internet Service Provider (ISP) established in 2000. Its core business is selling connectivity services (leased lines and ADSL) to the SME market, co-location space in their UK datacentres and domain registration and hosting services. They also sell cloud servers, currently on a VMware based platform and have developed a new, self-managing cloud platform based on the OpenStack hypervisor. 100 Percent IT is currently working on a Knowledge Transfer Partnership (KTP) with the University of Oxford to develop a Trusted Computing 'add-on' to OpenStack to allow for verifiably secure and auditable cloud solutions.

100 Percent IT mainly focus on the current cloud computing solution based on VMware, the OpenStack based cloud platform which is in alpha testing in house and the KTP enhancements to the OpenStack platform. The OpenStack platform is due to launch publically in Q1 2016 and will largely replace the VMware platform. It will be accessed directly by users through an online portal which will enable them to set up their account automatically, provision instances, configure many customisable networking features and monitor their usage levels. This will be aimed at both the SME market that typically will require single or tens of concurrent instances and which will typically be running for extended (years) periods and larger corporates and academic customers who typically will require high intensity services of several hundred instances for shorter periods. Customers set up their account online through the web portal and billing is automatically managed by the same system. Customers will pay for services via credit card and will automatically be billed for each recurring period of use.

100 Percent IT employs 4.5 full time people with the KTP associate plus several (currently 5) contractors and they have two staff with PhDs and two with Masters Degrees. 100 Percent IT is based in the Thames Valley in the south of the UK. The turnover for the financial year ending 30th June 2015 is predicted to be circa £380,000 (€530,000). Turnover once the OpenStack platform launches is anticipated to double annually.

3.6.2 Critical business process

Signing up customers (fraud checks, KYC[1])

This process is important for automated online transactions such as domain registration and hosting and cloud server provision. 100 Percent IT is developing this online capability, due to launch in Q1 2016. As sales will be made without human intervention, it is important for 100 Percent IT that customers are genuine and not exploiting their systems for fraudulent purposes. Example checks will

[1] Know Your Customer

include mobile contact number verification via SMS authentication and/or email address confirmation via a link which needs to be clicked prior to account acceptance.

Storage and processing of credit card details (PCI[2])

100 Percent IT has a merchant number and payment processing gateway provided by Global Payments. Specific PCI compliance checks must be passed to maintain this service and storage and processing of the credit card details for the automated payments of online accounts (see above) need to be adhered to both initially when setting up the payments and for ongoing continuous authority payments for recurring transactions.

Current Backup and disaster recovery

All cloud data is stored in Redundant Array of Independent Disks (RAID) with at least one redundant copy (normally two redundant copies). This data is snapshotted and replicated to another array on site as well as an offsite array every six hours. In the event of an array failure instances can be booted from the secondary array in the primary site with downtime limited to failure analysis plus instance boot time. In the event of a disaster taking out the primary site the backup site may have capacity to boot some servers instantly. Data stored there is mainly to protect against permanent data loss rather than provide instant failover.

Test data is created every six hours and an automated system verifies it is successfully replicated to the appropriate back up and disaster recovery locations. A system administrator is notified if this is not the case.

The OpenStack platform that is in final development follows a similar design but user data is stored simultaneously across multiple disk arrays in multiple racks to mitigate against an outage caused by an array failure and users have control of the number of backup copies that they maintain plus the backup location(s). Users also have the ability to boot instances from a DR copy themselves where system capacity and account usage limits allow.

Automated monitoring of infrastructure with notification both from within 100 Percent IT's own network and outside their network

Currently 100 Percent IT monitors every interface on the core routers, switches and firewalls every minute. CPU, memory and errors are logged on networking equipment to aid in diagnostic troubleshooting where required. Disk capacity, memory and CPU load are monitored on complete infrastructure. Customer-premises equipment (CPE) provided by 100 Percent IT is monitored typically for latency, packet loss and bandwidth usage. The configuration of all networking equipment is monitored and changes logged every 15 minutes. Cacti [48], Graphite [49] and Nagios [50] are used to display this graphically. Cacti is an open-source, web-based network monitoring and graphing tool designed as a front-end application for the open-source, industry-standard data logging tool: Round-Robin Database Tool (RRDtool). Graphite is a free open source software tool for monitoring and graphing the performance of computer systems. Graphite collects, stores, and displays time series data in real time. Nagios is an open-source application used to monitor systems, networks and infrastructure. Nagios offers monitoring and alerting services for servers, switches, applications and services.

[2] Payment Card Industry

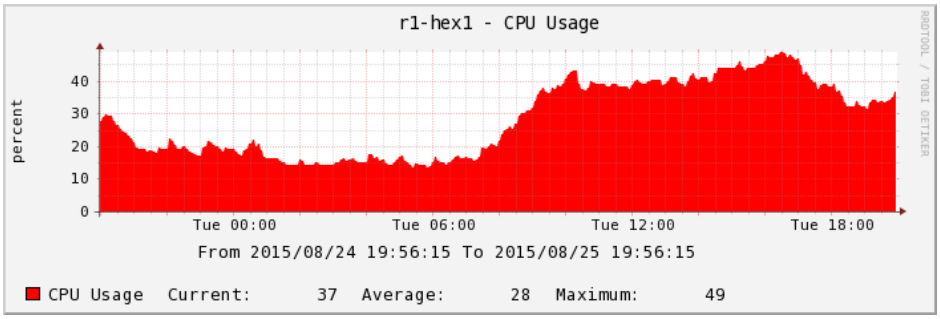

Figure 8: Example graph: 1CPU usage on a core router.

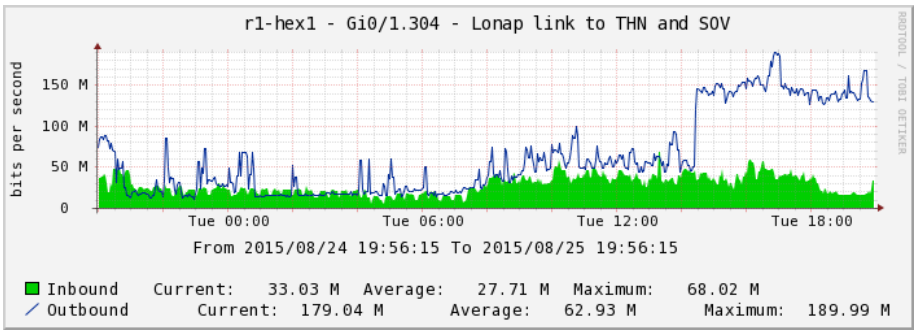

Figure 9: 2 Bandwidth in and out of a back-up interface for low priority traffic.

100 Percent IT also perform automated testing of systems that run across multiple servers such as email by having the testing platform use the service itself e.g. it will email itself every 15 minutes to check that all email systems are working correctly.

Infrastructure – tracking, testing and applying firmware updates, supplier warranties, spares

An automated configuration and orchestration system is used to deploy, configure and maintain all server infrastructures. This automatically ensures that servers are configured in the way that they are defined in the orchestration layer providing consistency and eliminating human error. The orchestration system allows 100 Percent IT to apply server updates in a rolling fashion to minimise disruption to end users and the length of the maintenance window. 100 Percent IT is integrating Trusted Computing into the orchestration system to ensure that the infrastructure cannot be tampered with without detection.

Software and firmware updates are tested in the lab environment prior to live updates which are scheduled for out of hours. Equipment in pairs is updated independently to prevent end user disruption. Essential infrastructure is covered by hardware warranties or self-insured with cold spares.

In house software – automated unit and integration testing, automated integration of bug fixes into production code and planning integration of new features into production code

Changes to any system code developed in house are always monitored by automated unit, functional and integration testing. When a programmer commits changes the system works out which program functions have been updated, automatically builds a new test cluster to check the changes have not broken anything and runs a series of tests against this test cluster before letting the programmer know

the result. These changes and test results are stored in the Gerrit code review platform so other members of the company can review and comment on them as appropriate.

Trusted computing – integration of 100 Percent IT's trusted computing extensions into OpenStack and VPN access

This is the development work being conducted in partnership with University of Oxford. 100 Percent IT is extending the OpenStack platform to allow Trusted Computing white listing and remote attestation. White listing is a system that ensures only programs that have been pre-authorised can run on the host or in an instance. Remote attestation allows users to ensure that their instance has not been tampered with by either a hacker or staff member of 100 Percent IT. This remote attestation feature is also being integrated in to a VPN client that will check the integrity of the instance before bringing up a connection thus preventing unintended data leakage as well as man-in-the-middle attacks. 100 Percent IT is working on integrating zero-knowledge encryption into the hypervisor which will mean that they can run user's instances and process their data while encrypted but will be unable to see their data – this will be especially useful for users in industries with stringent compliance requirements such as financial services. The trusted computing code will be certified by external verification bodies such as CESG/GCHQ.

100 Percent IT has equipment in four UK datacentres linked by 10G redundant links as per the network (see Figure 10). The data centre space and connectivity is outsourced to various suppliers. Redundant connectivity between the datacentres is provided by at least two independent suppliers across each site. Redundant transit and bandwidth links to external networks are in two UK datacentres with multiple transit links and peers in each.

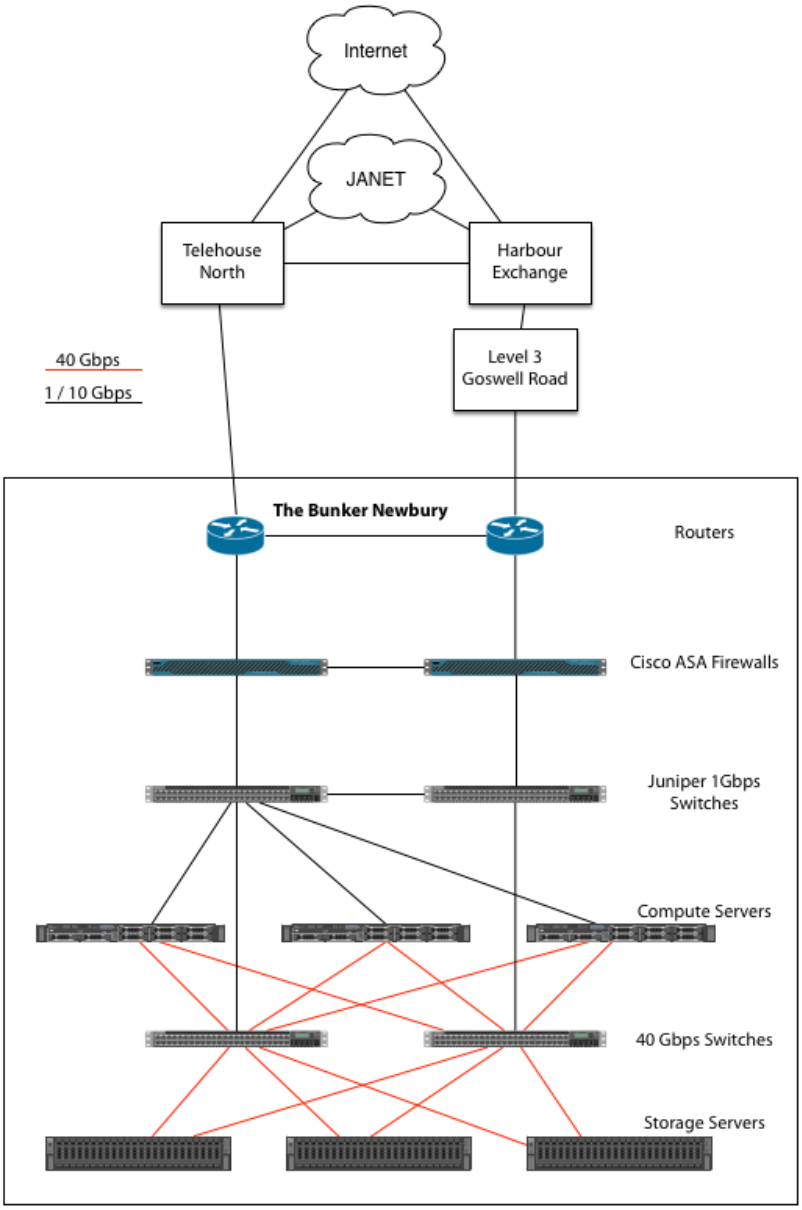

Figure 10: 100 Percent IT's cloud infrastructure.

Focusing on the cloud infrastructure, customer data is replicated both within a datacentre and offsite as described above. This gives protection against failure of a single piece of equipment in one data centre and a disaster recovery plan should an entire data centre go off line.

The new OpenStack system is extensively modified to include Trusted Computing as well as Multiprotocol Label Switching (MPLS) based software driven networking with local SSD storage in each compute node plus distributed storage based on a combination of SAS and SSD disks.

The Trusted Computing advantages have been described above.

This architecture allows the physical network to use a Clos system of routed point to point links rather than the normal layer 2 network between nodes. The reason for this is that each server has multiple links to multiple switches – if the network were layer 2 then each link would normally active/failover. More expensive switches supporting cross-chassis link aggregation are required to allow for active/active link usage. The layer 3 architecture uses the Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP) routing protocols to provide the advantages of:

- Full usage of all links in parallel across all switches with normal inexpensive layer 3 switches
- Easy cluster size increase by just adding switches that are automatically integrated after pasting in a configuration template
- Linear scalability of the system as adding switches increases the cross-sectional bandwidth between nodes (http://hsi.web.cern.ch/HSI/dshs/publications/rt97/html/node7.html)

The MPLS software driven networking system allows each customer to have one or more private networks with one or more private routers, firewalls or load-balancers that they can configure. MPLS and BGP are very well understood protocols that have been proven to scale across enormous numbers of users and their security has been well tested. All network traffic between instances is sent within the host to a virtual router and then MPLS switched directly to the destination host where is it passed on to the destination instance. Traffic in and out of hosts is hardware accelerated to minimise the increase in latency and maximise throughput and packets per second – current benchmarking has achieved 4.1 million packets per second between instances on different nodes compared to 0.5 million packets per second using normal OpenStack networking.

The architecture also allows 100 Percent IT to integrate hardware servers, firewalls and load balancers directly into a user's virtual network in a datacentre as well as integrate directly into a corporate user's physical MPLS network as either a routed or switched connection. This makes instances in the cloud appear to be on the user's company network.

The only drawback of the MPLS system is that it requires edge routers that support MPLS but 100 Percent IT uses these anyway in the rest of their business. According to 100 Percent IT, it was a little more difficult to build automated testing as they used to apply a hardware MPLS router with the test cluster, but now they have virtual routers that support MPLS so the system can be automated end to end. The underlying OpenStack systems have been modified to have no single point of failure and to support e.g. distributed multi-master SQL databases. This helps to both prevent downtime from the failure of a single node as well as making upgrades easier as one node can be taken offline at a time with no effect on end users. 100 Percent IT has added a billing system to OpenStack and integrated it into the web dashboard to allow users to see their current usage, historical usage and to pay invoices.

As well as distributed storage for instance volumes synchronously replicated across a single data centre 100 Percent IT uses the OpenStack Swift system to provide asynchronous replication across multiple data centres. This is useful for backup of user instances as well as for object storage as data in Swift is not vulnerable to an outage of a single data centre and gives users control of the number of backup copies of their data.

100 Percent IT currently uses SSH keys for access to servers and TACACS authorisation integrated with a central password store for access to network infrastructure. They are working on integrating hardware based two factor authentication using Yubikeys to supplement the strong passwords. Moreover, they use LastPass Enterprise to store passwords that need to be shared between users (e.g. for external web sites that do not support OAUTH) and to provide an audit trail of who has accessed these passwords.

100 Percent IT uses the software packages Logstash, Elasticsearch and Kibana to provide central logging of all logs from all infrastructure with automated alerting of matches against triggers they have defined. This makes is easy to see what is happening across all systems from a single web page and to correlate output from one system with that from another.

100 Percent IT uses the Python based system Odoo to store centralised customer details, Customer Relationship Management (CRM), accounts and support requests – this is easy to extend and integrate with other systems of 100 Percent IT such as OpenStack.

100 Percent IT provides a REST based API for resellers to register and maintain systems such as web hosting and domain registration.

Business processes are totally reliant on reliable infrastructure. Services run 24/7 and many are covered by a SLA with service credits due to end users for an outage that lasts more than 15 minutes. Service credits generally accrue at 100x the outage duration, capped at 50% of the total monthly costs. Direct financial impact is limited by the cap and set as a credit against future invoices to mitigate against customer loss due to the outage. Reputational damage is more important and drives the overall network design for the company which focuses on preventing downtime caused by equipment failure.

Business Process	Risk of Downtime	Impact of Downtime	Cost of Downtime
Cloud Server – failure of node in one Data centre	Medium – instances running on that node would be powered off and reboot on a different node.	Medium Low – instances automatically reboot on a different node.	Medium High – service credits may be due to users under SLA
Cloud Server – failure of one whole data centre	Low – data centre partners chosen with care with redundant power, ISO27001 etc. Issues are likely to be very short term (under 2 hours)	High – multiple customers affected.	High – service credits due to users under SLA.
Switch / Router failure	Low – all equipment specified in redundant pairs designed to withstand a single outage	Low – high. If only one of a pair fails, no impact to users but service vulnerable during outage. If both fail, high as multiple services affected until replacement hardware arrives	Low – High. No financial impact for single failure. SLA credits due to users if multiple failures causes outage
Connectivity – ADSL	Medium high – dependent on supplier's network and BT last mile	Low – usually affects only a few customers at a time.	SLA not provided for ADSL so no financial impact
Connectivity – Leased Lines	Medium Low – dependent on supplier network but business class service with SLA	Low – usually only affects one customer at a time	Medium – SLA may generate service credits.
Co-location	Low – Data centre partners chosen with care and with redundant power ISO27001 etc. Failure may be due to 100% switch failure or to customer's own hardware failure	Medium Low – data centre outage affects multiple customers but unlikely. Switch failure affects few customers but historically unlikely. Customer server failure not 100% IT's responsibility	Medium Low – SLA may generate service credits but backed by SLA from data centre.
Domain Registration / Hosting	Low – Service runs on cloud server infrastructure.	Medium – no new registrations possible during issue. Existing domains unlikely to be affected.	Medium – loss of business during outage.

3.6.3 Cybersecurity needs and current practice

Cyber incidents that could affect the business can be divided into those caused by **external factors outside the control of 100 Percent IT** such as DDoS attacks on the network and Hacking of systems and **internal factors** such as over-contention of the systems, customer data corruption and 'internal' customer hacking on the system or other customers. The overall objective is to maintain high availability of all services for customers and to minimise any reputational damage.

Threat	Mitigation
DDoS	Not considered a major threat at present as the company is not sufficiently well known to be a target. Future plans for mitigation when the risk balance justifies the expenditure include flow based analysis to automatically identify DDoS attacks and attempt mitigation using off load servers in house as a primary response. Offloading to cloud based DDoS prevention companies as a secondary response and black holing target customer IP addresses as a final response.
Hacking – 100 Percent IT's network	All network infrastructure is protected by firewalls limiting management access to a small range of local IP addresses accessible via a VPN for public access from a limited range of Public IP addresses. All equipment is further protected by strong passwords. All equipment firmware is kept up to date to mitigate known vulnerabilities. All access to the equipment from any source is logged and any configuration changes are automatically detected, stored in a central version control system and also emailed to a system administrator.
Hacking – customer data stored by 100 Percent IT	Customers are responsible for the software that they install on the IaaS instances provided by 100 Percent IT. This includes software patching of their operating system and applications. The functional network segregation discussed below prevents compromised customer systems affecting other customers directly or the 100 Percent IT infrastructure. Bandwidth limits on each customer prevent unexpectedly large bills caused by fraudulent activity and outbound emails will be capped to reduce IP address black listing. 100 Percent IT is currently developing software through the KTP integrating trusted computing into OpenStack which will prevent any software being run on either the hosts or guest instances unless it is on a pre-approved white list. This will mean that even if someone does manage to hack into a customer instance (usually due to application vulnerability or insufficiently strong user passwords) they cannot install unapproved or malicious software.
Over-Contention	Like all ISPs, 100 Percent IT operates services in a contended fashion. This enables them to offer excellent value to their users while not compromising performance. However it is vital that performance is closely monitored so that instances can be moved to other infrastructure should it prove necessary. Monitoring and migration of resources are automated. Results are also displayed graphically in the monitoring platform to allow system administrators to verify the current and historical system performance.
Customer data corruption (cloud servers)	To mitigate against corruption of customer data caused by a failure of the underlying storage provided by 100 Percent IT, all customer data is stored on a minimum of two disks. Customer data is check summed when saved and periodically scrubbed to compare the checksum against the data stored on disk. In the event that a checksum does not match the data is checked against the backup copies and automatically repaired if that copy is valid. If the other copies are invalid a system administrator is notified.
Protecting Cloud customers from other customers	100 Percent IT has modified OpenStack to use MPLS networking to give each customer a private network that cannot be accessed by or access other customer networks. Each customer has a private IP address range that can overlap with other customers but the networks are functionally separate preventing data leakage or attacks.
Protecting the	Customer's IP addresses do not have access to the management interfaces of

systems of 100 Percent IT from their customers	the infrastructure. They are treated as external and follow the protocols for external access discussed above.
Credit Card Details	100 Percent IT does not store credit card details. Instead they use tokenisation to have Authorise.net store the credit card details and they store a token which is used to debit the card when needed. This greatly reduces the PCI compliance requirements as if someone did manage to steal the tokens all they would be able to do is transfer money from customer cards into the account of 100 Percent IT, which is easily reversed.

100 Percent IT's team is currently too small to justify having dedicated person in charge of cyber risk and security.

Risk assessment of the cyber-infrastructure supporting critical business infrastructure is done every six months or when a new system or change is implemented. 100 Percent IT obtained ISO27001 certification which formalised these processes but certification was not renewed as customer demand did not require it. This will be reviewed again once the OpenStack Cloud platform is publically launched. Moreover, currently the company does not follow any established approach or standard for risk management or assessment.

Automated real-time monitoring of the infrastructure is in place, including bandwidth usage on multiple interfaces, and is monitored once per minute. This is primarily used to help debug customer network issues and to monitor expenditure over paid links however it also has uses in monitoring potential cyber-attacks. Unusual data spikes automatically raise support tickets. Data is stored in Cacti, Graphite and Nagios. Repeated invalid password attempts block the IP address requesting access and log the attempt.

As regards to recovery plans 100 Percent IT has concluded that the primary business disruption risk would be due to equipment failure or supplier failure. Disaster recovery plans and resilient network planning have been conducted with this in mind at all times. This automatically gives moderate protection against cyber-attacks as the source of attack is immaterial. The company has not specifically planned for a targeted attack that attempts to delete backups etc. in addition to the live data.

3.7 Friedrich Miescher Institute (FMI)

3.7.1 Organization and business goals

Friedrich Miescher Institute (FMI) is an academic research institute. The main goal of the institute is to produce high quality science, with a particular focus on biomedical research. FMI is a non-profit organization and is mainly funded by Novartis, which stands for 60% of the funding. The research groups in FMI publish articles targeting high-end, prestigious journals (high impact journals), typically one high impact paper per year per group. FMI has a very good publication ratio, which is higher than most academic institutions.

FMI has around 360 employees, divided in 23 research groups, where approximately 120 are students, 120 are post-docs, and 120 are permanent staff (including administration, technical platforms, technicians in groups, and group leaders). The administration is very small for the size of the organization and many financial and administrative services are outsourced to Novartis. Classic IT tends towards a headcount of approximately 5% for ICT from the total headcount, which would mean 15 people. At FMI there are only 7 persons in IT, so it is very lean. FMI has very competent staff to manage the IT infrastructure (2 sys admin), but external companies are used to do major software upgrades. Figure 11 shows the organizational structure of the IT department at FMI.

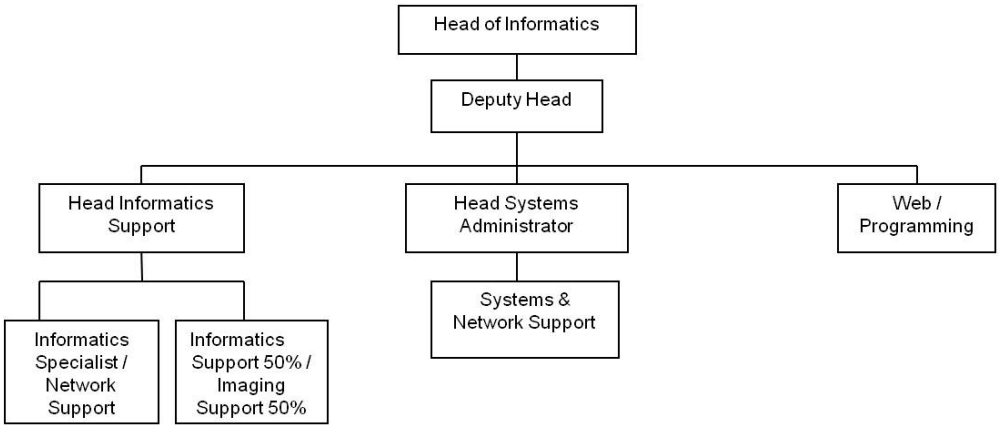

Figure 11: Organizational structure of the IT department at FMI

3.7.2 Critical business process

Network management is one of the most critical business processes in FMI. From a high level point of view, FMI has outsourced most of the HR and finance processes to Novartis, and some business processes, e.g. SAP, to two dedicated system administrators. FMI's stakeholders are the research groups, technical platforms, and administration. Storage server/network downtime can lead to researchers not being able to work. The impact of such incidents can be measured in lost working time (person hours).

Based on a previous survey, FMI IT Support received a 96% user satisfaction. FMI do not store any patient data, and all medical samples are completely anonymized. FMI do carry out animal studies and have approximately 20,000 mice for this purpose. Animal study data is considered sensitive because some groups in the public have a negative view towards animal research. There is a single mouse database that serves all the 23 research groups, which simplifies support and compliance to animal welfare laws.

The critical infrastructure is virtualized, which facilitates Disaster Recovery (DR) and backup. FMI do not use public cloud at the moment, they keep almost everything inside apart from non-critical items like web sites for the public, survey tools, etc. Private cloud is not needed as their needs are met by Virtual Machines (VMs). FMI runs a research infrastructure that is operative 24/7. They do not have Service Level Agreements (SLAs). It is assumed that the infrastructure is available 24/7. FMI claims that their good governance structure mitigates the need of an SLA (IT is managed by a steering board of research group leaders and technical platform heads).

They do not have any specific need for consent about security since most of the data will be eventually published and generally any security breach would affect one group. On the other hand, Novartis has high standards about IT security and expects FMI to develop similar standards, or at least adapt them to the FMI academic environment.

Researchers have administrator rights on their computers, which is a risk as they have the freedom to do whatever they need to do. However, the risk is balanced by the limited impact to a single group versus the benefit that they have freedom to test new tools and methods. In case of special needs they are assisted. They do have dedicated Virtual Private Network (VPN) and Demilitarized Zone (DMZ) they may use when connecting the Internet. However, internally, everything runs on the same network, though some management networks are separated. This is because the complexity that could be introduced is so high that they prefer to assume trust as overall risk is low.

All traffic going to the Internet goes over a proxy. The internal equipment is scanned for security vulnerabilities. Novartis cannot route in their network but the institute can route in Novartis network. There is a firewall to protect Novartis from the institute and a separate firewall for outside traffic. To summarize: FMI has one major critical IT business process, which is running the network.

As supporting infrastructure, FMI has a full disaster recovery plan across four data centres in place (two small data centres rooms at FMI and two Novartis data centre locations). The network is scanned internally using QUALYS scan to detect vulnerabilities. The connectivity between the data centres is very good and supported by fibre connectivity between each of the data centre locations and to the Internet.

In terms of capacity, the infrastructure has approximately 100 virtual machines (VMs), 1 Petabyte of data, 4 data centres, and approximately 1000 devices on the network. Tools provided by the company Veeam Software are used for automated backup and disaster recovery services for VMs. The data is backed up in two synchronous replicas of the database, and there are additional copies of the data in the datacentres. Independent from ICT security aspect, it is sometimes not possible to fully adopt information security policy from Novartis and policies need therefore to be adapted.

FMI's network is not accessible from outside. They have a firewall between them and Novartis, and an extranet with Novartis. Moreover, they do not have separation of the networks (e.g. VLANs). They do not allow connections of external entities to the local network. Nothing unmanaged by FMI should be on the network. FMI do not "punch holes" in the network; they have implemented Network Address Translation (NAT) and IP restrictions in some cases, and reverse proxy to some of the devices that researchers need.

If someone manages to get to Novartis assets via FMI network, it can entail such a compromised situation for FMI in terms of trustworthiness in the eyes of Novartis, who is their primary source of funding. FMI do not have penetration testing, which is required only on external-facing resources. Monitoring infrastructure is in place, which is made of several hundreds probes IT infrastructure, building infrastructure, and applications (based on Nagios monitoring).

There is a lot of flexibility for new employees (researchers). New employees are given admin rights to their own computer from the very start.

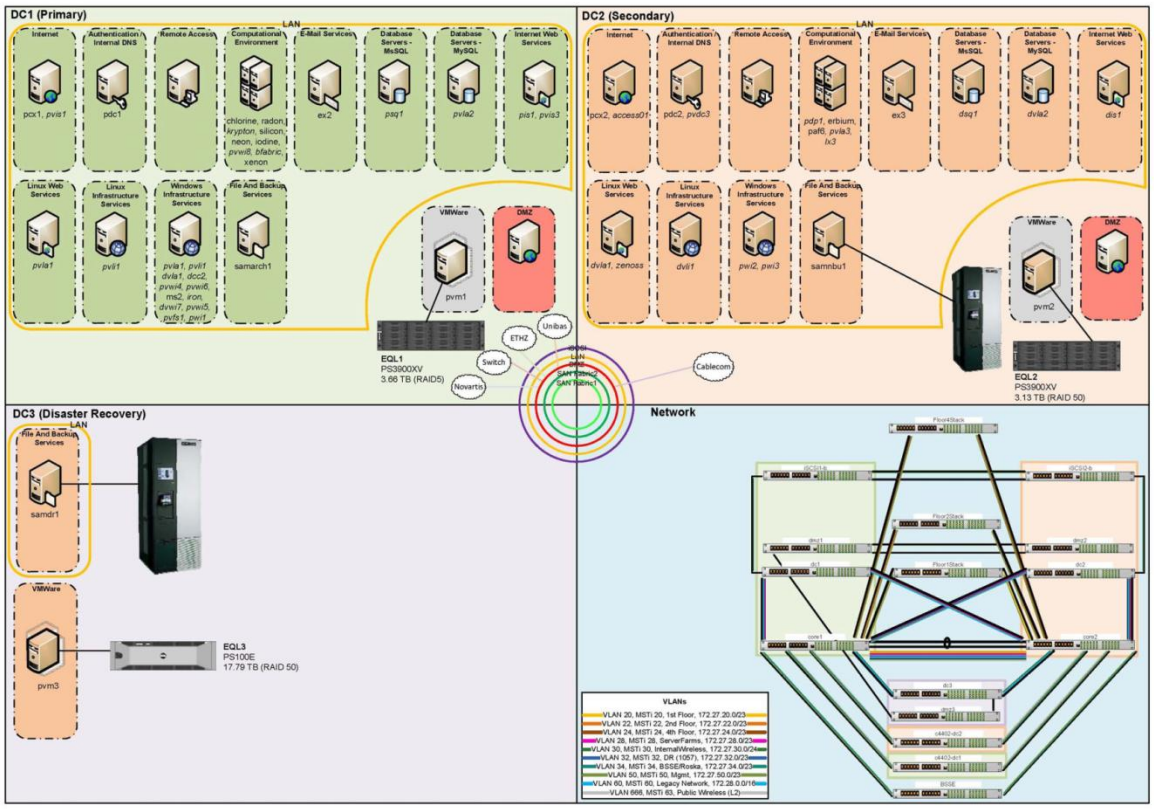

Figure 12: FMI network structure

3.7.3 Cybersecurity needs and current practice

The data stored in the databases is FMI's most important asset (that is, the 1 PB of data). However, approximately 10 TB may be regarded as mission critical. The mice database is probably the most sensitive database in terms of compliance and information about mouse lines. If FMI were to lose it, they would not be able to reconstruct know-how and information about the mice.

SQL injection is a kind of attack FMI would be really sensitive to. Everything in SW can be reconstructed. Cryptolocker [45] is an emerging threat. As FMI is segregated into different research groups it is likely that such an attack would largely impact one group based on security permissions. However, if administration is attacked it could be worse, but most critical data is kept in the Novartis SAP and HR systems. Another potential cyber risk regarded by FMI is the exploitation of the FMI infrastructure/system to access Novartis.

FMI does not have a dedicated person in charge of cyber risk/cyber vulnerability management, and does not currently conduct risk assessment of the cyber-infrastructure to support the critical business process. They are robust in information security risk management, but have no approach to cyber risk specifically.

FMI has a sophisticated risk management framework (which is the one utilized by Novartis), but it is an overall one (and high-level), and not just focused on IT security. This means that FMI does not follow any standard criteria as Novartis, but they have their own testing processes.

FMI does not have any kind of automated real-time monitoring of the cyber-infrastructure in place to detect attacks or incidents. However, because of their normal recovery plans, they are able to recover from damaging consequences of cyber-attacks. Moreover, FMI has two independent Internet providers. They use DNS from external service, and do not use Border Gateway Protocol (BGP) - they do use external DNS services with failover to the second network.

Confident of being fairly resilient against cyber risk, but they are aware of the fact there is not such a thing as “zero cyber risk”

3.8 Mare Beach Wear

3.8.1 Organization and business goals

Marebeachwear (www.marebeachwear.com) is an online Italian Luxury Beachwear Store. Its mission profile is to promote and distribute all around the world "the best beachwear that is made in Italy".

The perhaps more unique aspect of Marebeachwear's value proposition is to choose very small manufacturers that are more like "artisans of luxury beachwear" (and, by definition, unable to reach for global visibility) and promote them globally, through their sophisticated web platform, integrated with campaign management, order management and digital strategy (including social media).

Currently, Marebeachwear proposes 9 Italian brands. Marebeachwear has also a physical point of sale, located in Treviso (Italy). The shop has the physical warehouse and is the hub for all parcels in and out (pick-up and drop-off location). The long-term ambition of Marebeachwear is to develop and commercialise a Marebeachwear-branded product line.

Marebeachwear is a very small SME, with 4 people in total. It was launched in May 2013, and is still in its start-up phase, with a rapidly growing turnover (but still <1M€).

3.8.2 Critical business process

With respect to supply chain, purchases for the Spring-Summer collection 2016 are conducted offline between June and August 2015. This introduces a weakness in the model, as re-orders are typically not possible, given the made-to-order approach taken by the suppliers.

The web-platform management is partly insourced (through an evolved Content Management System (CMS): content and catalogue updates), the rest is outsourced. The ticketing system is in place with the ICT strategic supplier. Moreover, marketing and communication is partly outsourced.

The process is partly on the Marebeachwear platform (first steps of the process) and partly on the UPS platform (light integration), including the parcel-tracking procedure. After-sales is handled from the physical point of sale and integrated on the web platform. Marebeachwear uses Sella Bank as online payment system.

The web services are managed with a full outsourcing approach. The e-commerce platform is hosted in a Virtual Machine placed in an infrastructure based on a virtualised solution on top of 3 ESX servers, each equipped with (2 CPU quad-core; 24GB RAM; VMWare enterprise 4.1; Hard disk 1,5TB, 34 Mbps Internet access). The 3 servers are interconnected with 1 SAN AX4 dedicated for storage (HDD in RAID5 configuration to guarantee fault tolerance). The available infrastructure also consists of 4 Switch, 1 Router/Firewall CISCO, 1 SMTP physical server, 1 OPENVPN physical server. The Backup solution is based on server located in a different location and equipped with CPU Intel® Core™ i7-3930K Hexacore incl. Hyper-Threading Technology, RAM 64 GB DDR3 RAM; Hard disks 2 x 3 TB SATA 6 Gb/s HDD 7200 rpm (Software-RAID 1), NIC 1 Gbit connected at 100 Mbit, 100 GB Backup Space. Figure 13 illustrates the server infrastructure.

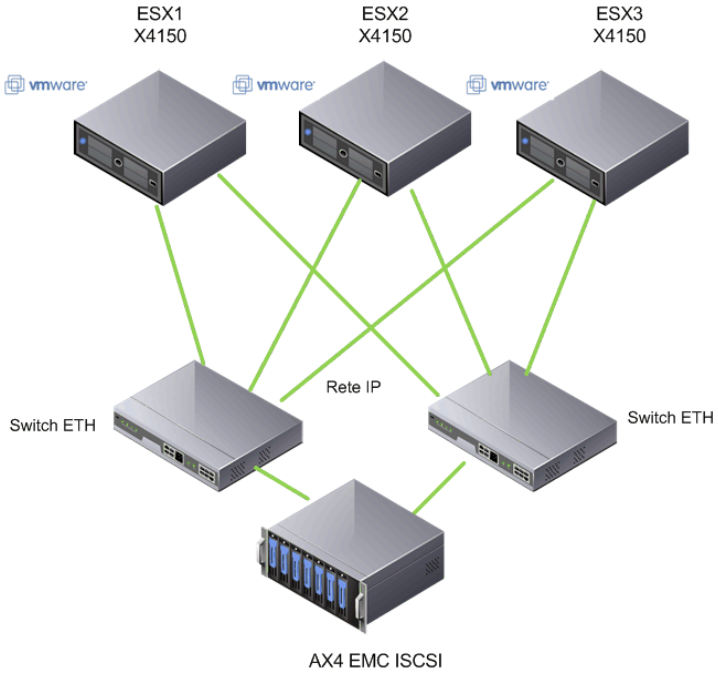

Figure 13: Server infrastructure

The critical business processes depends highly on the expected behaviour of the ICT infrastructure. In fact, the online shop is the core of the business model and its downtime has direct repercussions on the Company's turnover (1 day of downtime indicates 1/365 less turnover, which is even higher during peak season), as well as the reputation of the company.

3.8.3 Cybersecurity needs and current practice

Marebeachwear's most important assets are the customer database, the catalogue, warehouse information on goods assortment etc., and images and news published. The database consists of login, password, address, discount campaign, as well as a loyalty program with accumulation of "shells" to be reused for discounts or access to special services. However, there is no Customer Relation Management (CRM) in place. With respect to the catalogue, Marebeachwear has about 500 SKUs and they do not have an alerting system in case of malicious alteration, for instance, of the

prices or other crucial info, they would have no way of immediately knowing that there was something wrong.

Marebeachwear does not have dedicated persons in charge of cyber risk/cyber security and has outsourced this to the IT provider. However, there are no specific clauses regarding this in the SLAs that are established between Marebeachwear and the IT provider.

Marebeachwear has never conducted a risk assessment of the cyber-infrastructure prior to WISER's EAP. The web platform is monitored by a supervisory system, active 24/7, that checks the correct and effective functioning of the CMS installed every 5 minutes; in case of malfunctioning, the system automatically sends a message to an assistance service.

To support recovery in case of damage as a consequence of cyber-attacks, daily backups are performed (and for critical services even hourly backups) maintaining a history of previous weeks. To ensure even more security, backups are performed and stored in different geographic locations to be used in case of disaster recovery. In case of damage on software and data the provider is able to restore the platform to a previous functioning point in a few hours. However, no cyber-attack specific plan is in place.

4 Common needs and challenges among the associate partners

The descriptions from Section 3 shows that the associate partners represent a very diverse group of businesses and domains, including biomedicine and biomedical research, health care, transportation, bioinformatics, ICT services, fashion, and oil & gas. However, there are a number of concerns that are shared by more or less all of them. All associate partners rely to a high degree on interconnected ICT infrastructure for their critical business processes. The services supported by this infrastructure and the data stored or handled are not just something that helps the businesses to operate more efficiently than would otherwise be possible, but are core prerequisites for the businesses to run at all. Switching to "manual or paper mode" or going offline for any considerable amount of time is rarely an option. Protecting the ICT infrastructure from attack and ensuring the continuous availability and integrity of services and data is therefore essential. For all the associate partners, loss or disruption of the ICT infrastructure may prevent them from running critical business processes and lead to significant economic loss. For some of those involved in the medical and safety domains, it could, in the extreme worst case, even lead to loss of life.

Many of the associate partners store or handle sensitive data of one kind or another on their ICT infrastructure. Such data relate, for example, to patient health and medical issues. Revealing such data to unauthorized entities could not only cause harm and distress for the affected patients, but also lead to fines or other reactions from the authorities. Other data relate to inside business information which could be taken advantage of by competitors or even criminals, and also affect stock prices if revealed. Ensuring the confidentiality of sensitive data is therefore a central common concern.

For most of the associate partners, their reputation among their clients and the society in general depends to a very large degree on their ability to protect themselves against cyber attacks. If incidents leading to significant service disruption or confidentiality breaches occur and are revealed, it may have a devastating effect on the clients' trust and organization's standing among the public. Such occurrences could therefore lead to loss of customers and threaten the partner's ability to successfully remain in business.

The maturity level and ways in which cyber security and risk management is handled varies widely among the associate partners. This is not surprising, as they differ a lot with respect to business domain, size and organization. Few of them have large resources set aside specifically to deal with cyber security and risk management. In this respect, it seems reasonable to assume that the combined group of associate partners reflects fairly well the general state of European small and medium businesses. In several cases, a single individual is assigned responsibility for cyber security as a part-time task in addition to other daily duties, or the responsibility is shared among a group of employees in a more or less informal manner.

Most associate partners perform some kind of risk assessments or audits. For some, this is done periodically, typically once a year. Others do it on an ad-hoc basis, for example when new products are released or new clients or customers are introduced. Some of the partners use standards such as ISO 31000 or ISO 27001 to support the risk management activities, without necessarily claiming strict adherence. One associate partner is certified for ISO 13485. This standard is concerned with quality management for medical devices but addresses also risk, although not with special focus on cyber risk.

Most associate partners also report that they have recovery and response plans in place in case of a cyber incident. Typically, this involves quickly replacing/reinstalling compromised parts with clean backup versions and analyzing the cause of the incident in a safe environment. In one case, the response plan also allows the possibility of temporarily switching to paper-based operation of critical processes while the system is recovered. However, most response plans seem to provide little or no guidance on tailoring the response to the estimated risk level as viewed from the overall business perspective. Hence, there is a possibility that the response does not match the risk. For example, a response that is costly in terms of money, resources or customer satisfaction may be initiated even for a small risk with acceptable consequences.

Some of the associate partners have tools in place for detecting vulnerabilities and/or monitoring the ICT infrastructure for suspicious activities and indications of a cyber attack. None of them report that they explicitly link results from these tools to the overall risk picture for the organization. This means that it can be challenging to know how the low-level technical information obtained from the tools affects the more business-oriented risk picture for the organization. Moreover, it does not ensure that the risk picture is up to date with respect to the latest monitoring results.

From the EAP descriptions in Section 3 and the summary above, it is clear that all associate partners depend on effective protection of availability, confidentiality and integrity of data and services in order to carry out their critical business processes in a satisfactory manner. A central hypothesis of WISER, which helps guide the framework design and requirements capture, is that the following will significantly contribute to such protection:

- Monitoring tools that are able to quickly detect indications that a cyber attack might be under way and to provide early and appropriate warnings so that suitable action can quickly be taken to avoid or minimize damage to the organization's services and data.
- An updated risk picture with support for understanding what risks and consequences are related to a detected or suspected attack. This needs to be considered not only at the detailed technical level, but also in the larger perspective of the organization and its business, including customers and clients. In some cases, societal impact could also be relevant, for example in relation to safety for petroleum installations or preventing organized crime at a port.
- Support for selecting appropriate responses and mitigation options for detected or suspected attacks and corresponding risks. This should help the user to choose a suitable response based on weighing the cost against the benefits, taking into account the business perspective of the organization, and possibly also societal considerations, rather than purely technical issues.
- Last, but not least, it is vital that the framework do not necessarily require extensive resources or highly specialized skills to be put into use. Indeed, this would prevent most of the associate partners from adopting the methods and tools offered by the framework, thereby to a large degree defeating its intended purpose. For organizations with limited resources it should be easy to adopt and configure the framework in a generic manner from simple guidelines and patterns, although this will of course limit the specificity of the assessments with respect to the individual organization. This type of application of the framework would likely be the most relevant for the majority of the associate partners. Notice, however, that other kinds of organizations will want a more advanced application specialized towards their own organization and business context.

5 Best practice: Standards and methods for risk management

In this section we give an overview over standards, methods and best practices for security risk management and security risk assessment. We focus in particular on standards provided by the International Organization for Standardization (ISO) and the National Institute of Standards and Technology (NIST) as they are well established and widely used.

5.1 Overview of relevant ISO/IEC standards

The following standards provided by the International Organization for Standardization (ISO) and the International Electrotechnical Commission are relevant within the scope of WISER.

- ISO/IEC 31000, Risk management – Principles and guidelines [14].
- ISO/IEC 31010, Risk management – Risk assessment techniques [15].
- ISO/IEC 27001, Information technology – Security techniques – Information security management systems – Requirements [16].
- ISO/IEC 27005, Information technology – Security techniques – Information security risk management systems [17].
- ISO/IEC 27032, Information technology – Security techniques – Guidelines for cybersecurity [18].

Figure 14 illustrates the relationship between the above mentioned standards. Generic standards are represented in light-grey boxes while standards related specifically to cybersecurity are represented in white boxes.

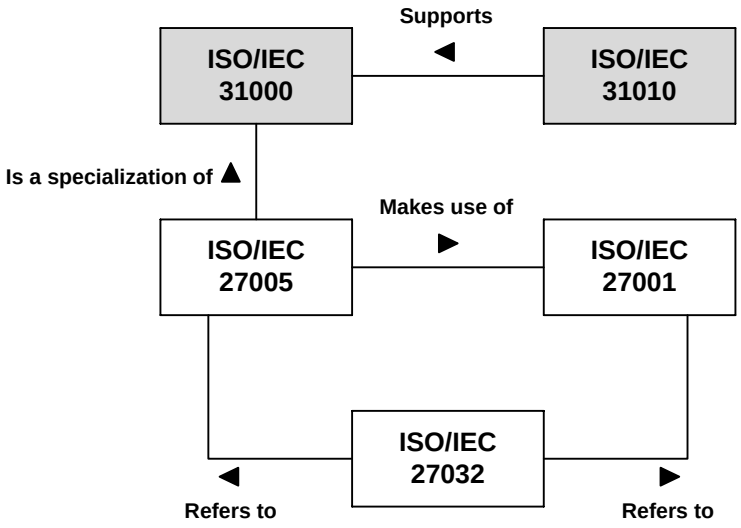

Figure 14: The relationship between relevant ISO/IEC standards

ISO 31000 provides generic guidelines on risk management. ISO 31010 is a supporting standard for ISO 31000 and provides guidance on selection and application of systematic techniques for risk assessment. ISO 27005 is a specialization of ISO 31000 in the sense that it adjusts the generic guidelines in ISO 31000 to focus specifically on security. ISO 27005 provides guidelines for information security risk management in an organization, supporting in particular the requirements of an information security management system according to ISO 27001. ISO 27032 provides high-level technical guidance for addressing common Cybersecurity risks, and refers to a set of standards and best practices for detailed technical guidance, including ISO 27005 and ISO 27001.

In the following sections we present the abovementioned standards. ISO 31010 is presented in the context of ISO 31000.

5.2 ISO 31000 – risk management – principles and guidelines

The international standard ISO 31000 provides principles and generic guidelines on risk management. Due to its generic nature, the standard is not addressing any specific kind of risk and is not specific to any industry or sector, but rather points out that it may be used by anyone (ranging from an individual to a national organization) and may be applied to any type of risk. Moreover, the standard does not only consider the potential loss resulting from risks, but also the potential gain resulting from risks. The standard also points out that it does not intend to promote uniformity of risk management across organizations, and that the design and implementation of risk management plans and frameworks will need to take into account the varying objectives, operations, assets, etc. of a specific organization.

As illustrated in Figure 15, the risk management process provided by ISO 31000 consists of five steps: (1) context establishment, (2) risk assessment, (3) risk treatment, (4) monitoring and review, and (5) communication and consultation.

The purpose of Step 1 is to describe the objective, define parameters to be taken into account when managing risk, and setting the scope and risk criteria for the remaining steps in the process. The purpose of Step 2 is to identify, analyse, and evaluate risks. Risk identification involves identifying sources of risk, areas of impact, events and their causes. According to ISO 31000, the aim is to identify a set of risks based on the events that may create, enhance, prevent, degrade, accelerate, or delay the achievement of objectives. Risk analysis involves identifying the positive or negative consequences of the identified risks, as well as the likelihood that those risks can occur. Risk evaluation involves identifying the criticality (risk level) of identified risks by mapping their consequence-likelihood combination to a set of predefined risk evaluation criteria. The aim is to prioritize risks and assist decisions about which risks to treat. The purpose of Step 3 is to select one or more options for modifying risks, and implementing those options. The purpose of Step 4 is to ensure that controls are effective and efficient in both design and operation, obtain information to improve risk assessment, detecting changes in the risk picture and to identify emerging risks. The purpose of Step 5 is to communicate and consult with external and internal stakeholders during all stages of the risk management process. As illustrated in Figure 15, Steps 4 and 5 are carried out continuously throughout the risk management process.

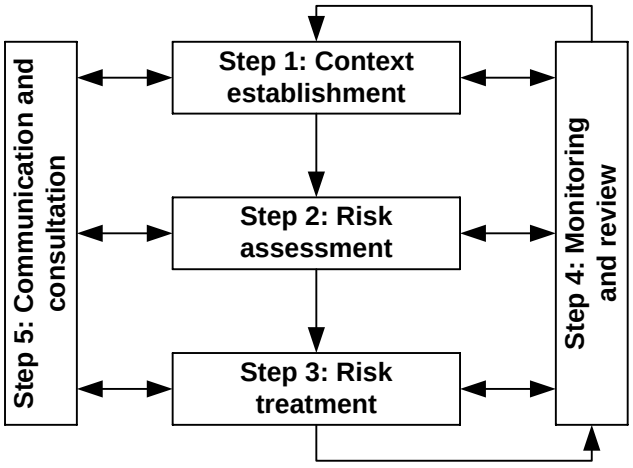

Figure 15: Risk Management Process (adapted from ISO 31000)

ISO 31010 is a supporting standard for ISO 31000 and provides guidance on selection and application of systematic techniques for risk assessment. The standard focuses on risk identification, risk analysis, and risk evaluation, and explains how each of these steps should be carried out. Then, the standard provides a list of specific tools and techniques and explains to what degree they are applicable for risk identification, analysis, and evaluation. With respect to risk analysis, the tools are further categorized in terms of applicability for consequence analysis, probability analysis and risk level analysis.

5.3 ISO 27001 – information technology – security techniques – information security management systems – requirements

ISO 27001 provides a process for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System (ISMS). The process adopts a so-called "Plan-Do-Check-Act" model, which is applied to structure all ISMS processes. Figure 16 illustrates the process.

According to ISO 27001, the purpose of the "Plan" phase is to establish the ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security. The aim is to deliver results in accordance with an organization's overall policies and objectives. The purpose of the "Do" phase is to implement and operate the ISMS policy, controls, processes and procedures. The purpose of the "Check" phase is to assess and measure the performance ISMS processes against ISMS policy, objectives and practical experience. The results are reported to management for review. Finally, the purpose of the "Act" phase is to achieve continual improvement of the ISMS by taking actions based on the results of the "Check" phase, as well as the management review.

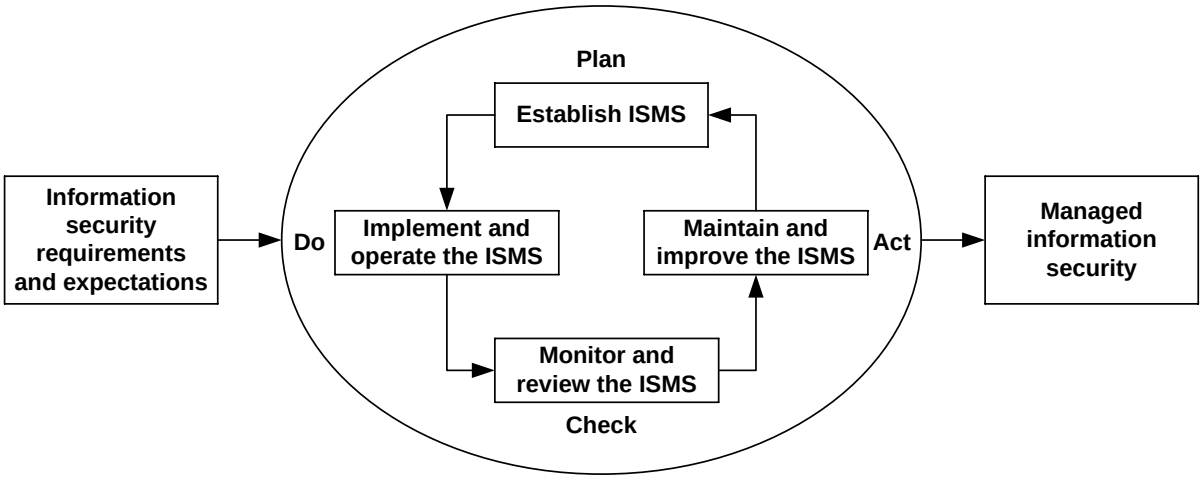

Figure 16: The ISMS process (adapted from ISO 27001)

5.4 ISO 27005 – information technology – security techniques – information security risk management

ISO 27005 provides guidelines for information security risk management. ISO 27005 supports the general concepts specified in ISO 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach. Thus, the guidelines provided by ISO 27005 are in line with ISO 31000 as reflected in Figure 17. Similar to ISO 31000, the information security risk management process is generic and may be applied to an organization as a whole, any discrete part of the organization, any information system, or existing/planned/particular aspects of control.

The security risk management process provided by ISO 27005 differs slightly from the general risk management process provided by ISO 31000: ISO 27005 put more emphasis on iterating the risk assessment process, as well as the risk treatment activities. This is reflected in Figure 17. ISO 27005

points out that an iterative approach to risk assessment can increase depth and detail of the assessment at each iteration, as well as supporting the identification of treatments more efficiently.

The process is as follows. First, the context is established. Second, a risk assessment is conducted (with a particular focus on security). Third, if the security risk assessment provides sufficient information to effectively determine the actions required to bring risks to an acceptable level then the task is complete and risk treatment is initiated. However, if the information is insufficient, another iteration of security risk assessment is conducted based on revised context and scope.

If the treatments do not immediately lead to an acceptable level of (residual) risk then another iteration of the risk assessment with changed context parameters may be required, followed by risk treatment.

The purpose of the risk acceptance (Step 4) is to ensure that risks are explicitly accepted by the managers of the organization. This is in particular important if the implementation of security controls is omitted or postponed because of cost. The purpose of the remaining steps is similar to the purpose of the steps in the risk assessment process provided by ISO 31000, with a particular focus on security.

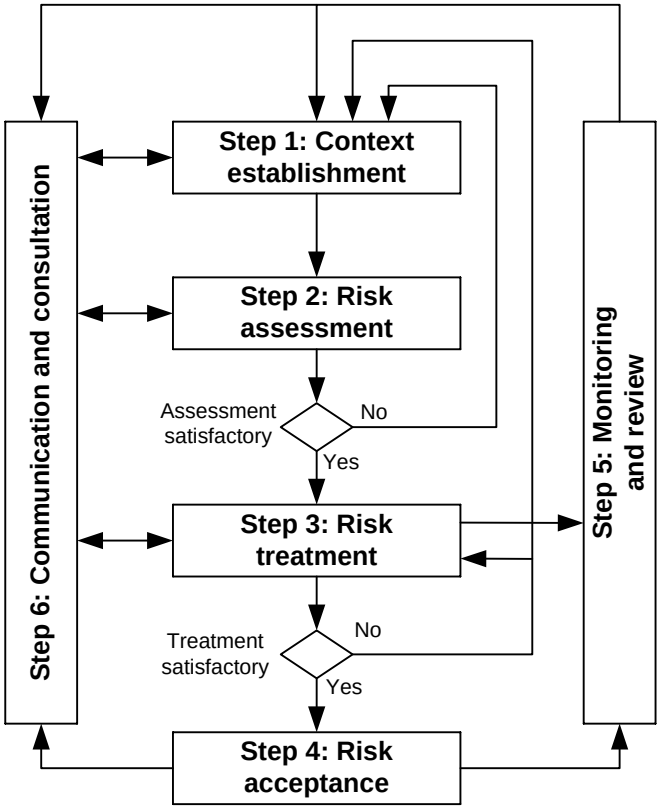

Figure 17: Security risk management process (adapted from ISO 27005)

5.5 ISO 27032 – information technology – security techniques – guidelines for cybersecurity

ISO 27032 focuses on two main areas. The first area of focus is to address Cybersecurity issues with a particular emphasis on bridging the gaps between the different security domains in the Cyberspace. The second area of focus is collaboration amongst stakeholders in the Cyberspace.

To support the first area of focus, the standard provides high-level technical guidelines for addressing common Cybersecurity risks such as hacking, malicious software, and spyware, and identifying appropriate security controls. To support the second area of focus, the standard provides a framework

for secure and reliable information sharing, coordination, and incident handling. The framework includes key elements of considerations for establishing trust, necessary processes for collaboration and information exchange and sharing, as well as technical requirements for systems integration and interoperability between different stakeholders.

The topics covered by the standard, in the above context, are as follows.

- Stakeholders in the Cyberspace
- Assets in the Cyberspace
- Threats against the security of the Cyberspace
- Roles of stakeholders in Cybersecurity
- Guidelines for stakeholders
- Cybersecurity controls
- Framework of information sharing and coordination

5.6 Overview of relevant NIST standards

The following standards provided by the National Institute of Standards and Technology (NIST) are relevant within the scope of WISER.

- NIST Framework for Improving Critical Infrastructure Cybersecurity [19].
- NIST Special Publication 800-39, Managing Information Security Risk – Organization, Mission, and Information System view [20].
- NIST Special Publication 800-30, Guide for Conducting Risk Assessment [21].
- NIST Special Publication 800-37, Guide for Applying Risk Management Framework to Federal Information Systems – A Security Life Cycle Approach [22].
- NIST Special Publication 800-60 Volume 1, Guide for Mapping Types of Information and Information Systems to Security Categories [23].
- NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations [24].
- NIST Special Publication 800-53A, Assessing Security and Privacy Controls in Federal Information Systems and Organizations [25].
- NIST Special Publication 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations [26].

Figure 18 illustrates the relationship between the above mentioned standards.

The NIST Cybersecurity Framework provides a collection of standards and best practices in order to help organizations manage cybersecurity risks, including NIST 800-39 and NIST 800-53. NIST 800-39 provides an overall security risk management process, similar to ISO 27005, and is the flagship document in the series of information security standards and guidelines developed by NIST. The overall process provided by NIST 800-39 consists of four main steps: (1) risk framing, (2) risk assessment, (3) risk responding, and (4) risk monitoring. In the context of WISER, the most relevant steps are Steps 2 and 4. NIST 800-30 explains in detail the risk assessment process introduced in NIST 800-39, while NIST 800-137 presents in detail guidelines for (continuous) risk monitoring.

NIST 800-37, on the other hand, provides an overall risk management framework. The framework is supported by the risk management process provided by NIST 800-39. The framework is presented in terms of a security life cycle consisting of six steps: (1) categorize information systems, (2) select security controls, (3) implement security controls, (4) assess security controls, (5) authorize information systems, and (6) monitor security controls. In the context of WISER, the most relevant

steps are Steps 1, 2, 4, and 6, which are explained in detail by NIST 800-60, NIST 800-53, NIST 800-53A, and NIST 800-137, respectively.

NIST 800-37 supports NIST 800-60 in sense that the results of risk monitoring may be used as a basis for repeating the risk management framework security life cycle. The aim is to identify and implement appropriate security controls as a response to the findings reported by risk monitoring.

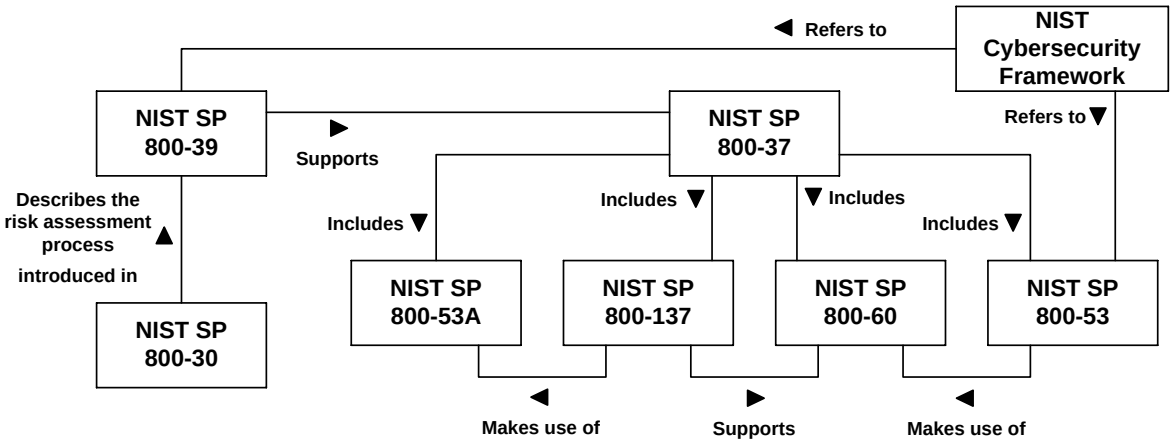

Figure 18: The relationship between relevant NIST standards

In the following sections we present the abovementioned standards. NIST 800-137 (risk monitoring) makes use of the guidelines provided by NIST 800-53A (security control assessment). NIST 800-53A is therefore presented in the context of NIST 800-137. NIST 800-53 (security control selection) makes use of guidelines provided by NIST 800-60 (information systems categorization). NIST 800-60 is therefore presented in the context of NIST 800-53.

5.7 NIST framework for improving critical infrastructure cybersecurity

The NIST Framework for Improving Critical Infrastructure Cybersecurity is a set of industry standards and best practices organized with respect to five main activities to help organizations manage cybersecurity risks. The framework has been created through collaboration between government and the private sector. NIST explicitly states that the framework is not designed to replace existing processes, but should rather be used by organizations as a tool to establish a new cybersecurity risk management process, improve an existing process, or express cybersecurity requirements to business partners and customers. Moreover, the framework also provides a general set of considerations, in terms of privacy and civil liberties, which needs to be taken into account as part of a comprehensive cybersecurity risk management process.

The framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. The framework consists of three main parts: the framework core, the framework implementation tiers, and the framework profile.

The Framework Core represents the five main activities (referred to as functions) in the framework: Identify, Protect, Detect, Respond, and Recover. These functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk. Each function is further refined into a set of categories, which basically describe various desired outcomes for each function. Each category is then refined into a set of subcategories which describe in more detail the desired outcomes. Finally, each subcategory is associated to a set of informative references, that is, standards and best practices, which may be used as a means to achieve the desired outcomes.

The Framework Implementation Tiers define four levels of rigor and sophistication describing the degree to which an organization's cybersecurity risk management practices exhibit the characteristics

defined in the Framework. Tier 1 represents the lowest level of rigor and sophistication, while Tier 4 represents the highest level. These tiers are supposed to help organizations to understand their current level of rigorousness and sophistication, and what is required to achieve a higher level. Although organizations identified as Tier 1 are encouraged to consider moving toward Tier 2 or greater, tiers do not represent maturity levels. Thus, an organization should determine and select a desired tier with respect to organizational goals, implementation feasibility, and whether the selected tier reduces cybersecurity risk to levels acceptable to the organization.

The Framework Profile is the alignment of the functions, categories, and subcategories with the business requirements, risk tolerance, and resources of an organization. Organizations may define profiles by comparing their current practice with the functions, categories, and subcategories in the framework. The profile may then help organizations identify possible gaps between their current practice and the best practices suggested by the framework. Thus, a profile enables organizations to establish a roadmap to achieve desired level of rigor and sophistication with respect to cybersecurity risk management practices. The framework does intentionally not provide profile templates to allow for flexibility in the definition and implementation of a profile.

Figure 19 is taken from The NIST Framework for Improving Critical Infrastructure Cybersecurity and illustrates the five functions in the framework, the decomposition of functions into categories, which are further decomposed into subcategories. The subcategories are then related to informative references.

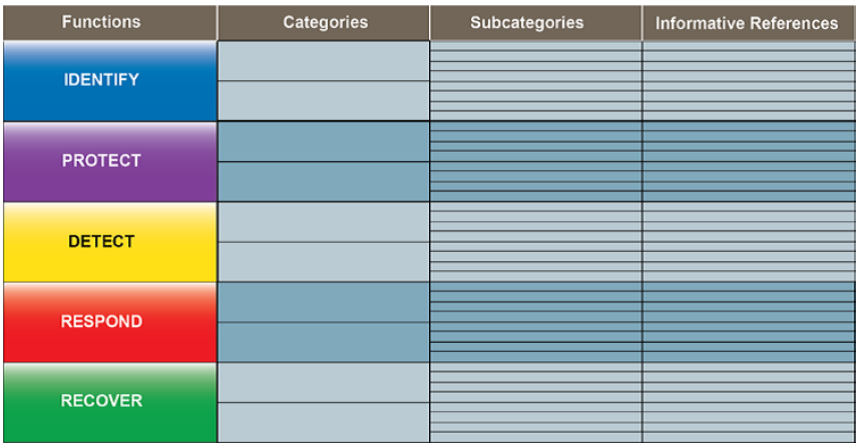

Figure 19: NIST Cybersecurity Framework

5.8 NIST 800-39 – managing information security risk

NIST 800-39 is the flagship document in the series of information security standards and guidelines developed by NIST. The purpose of NIST 800-39 is to provide guidance for an integrated, organization-wide program from managing information security risk, supported by a generic process for assessing, responding to, and monitoring risk on an ongoing basis. NIST 800-39 is supported by other NIST security standards and guidelines, including NIST 800-30 and NIST 800-53. In addition, it is also supported by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) standards ISO/IEC 31000 and ISO/IEC 27005. However, NIST 800-39 extends these international standards to particularly support the federal government and its contractors.

The risk management process consists of four main steps: (1) risk framing, (2) risk assessment, (3) risk response, and (4) risk monitoring. Each of these steps consists of a set of sub-steps. The purpose of Step 1 is to establish the context in which risk-based decisions are made, and to produce a risk management strategy that addresses how to assess risk, respond to risk, and monitor risk. This includes identifying risk assumptions (for example, assumptions about threats, vulnerabilities, and consequence/impact), risk constraints (for example, constraints related to the risk assessment), risk

tolerance (for example, risk acceptance criteria), and priorities and trade-offs (for example, trade-offs between different types of risks).

The purpose of Step 2 is to identify threats, internal and external vulnerabilities, the consequence/impact that may occur given the potential for threats exploiting vulnerabilities, and the likelihood that harm will occur. Based on this, risk is determined with respect to consequence and likelihood of harm occurring.

The purpose of Step 3 is to provide a consistent, organization-wide, response to risk in accordance with the organizational risk frame (defined in Step 1). This is carried out by developing, evaluating, and determining appropriate courses of action for responding to risk, and then implementing risk responses based on selected courses of action.

The purpose of Step 4 is to monitor risk over time in order to: verify that planned risk countermeasures (risk responses) are implemented and that information security requirements are satisfied, determine the effectiveness of the risk countermeasures, and identify changes to the information system and its environment that may have an impact on risk.

Figure 20 illustrates the risk management process described above. The nodes in the figure represent the four steps in the process, while the arrows in the figure represent the information and communication flow in the process. The bidirectional nature of the arrows indicates that the information/communication flow between the steps, as well as the execution order of the steps, may be flexible to reflect the dynamic nature of the risk management process.

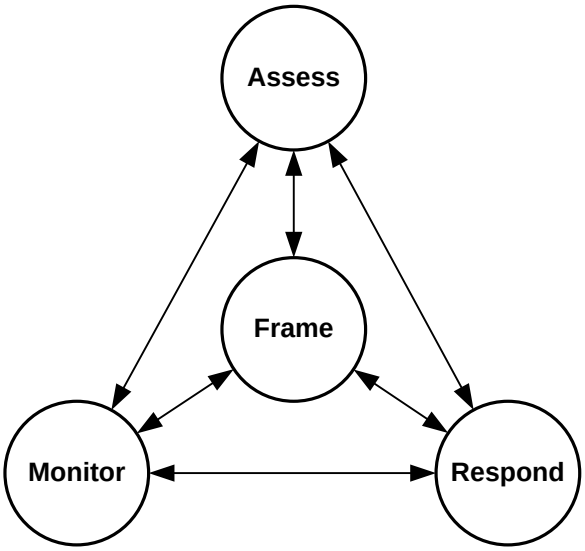

Figure 20: Risk Management Process (adapted from NIST 800-39)

5.9 NIST 800-30 – gudie for conducting risk assessment

The NIST Guide for Conducting Risk Assessments (NIST 800-30) provides a process to conduct risk assessment of federal information systems and organizations, with a particular focus on security. The suggested process and related concepts are intended to be in line with the risk assessment processes provided by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) standards, for example, ISO 31000 and ISO/IEC 27005. However, NIST 800-30 states that it extends the concepts and principles of these international standards to particularly support the federal government and its contractors. Moreover, NIST 800-30 argues that risk assessments are traditionally carried out at the level of information systems, and therefore tend to overlook important risk factors that may be more appropriately assessed at the organizational and mission/business process level. To address this, NIST 800-30 suggests conducting risk assessment at the organizational level (Tier 1), mission/business process level (Tier 2), and information system

level (Tier 3), and explains the benefit of risk assessment in each level and how the results complement each other.

According to NIST 800-30, the results of a Tier 1 risk assessment may support decisions affecting, for example: organization-wide information security programs, policies, procedures, and guidance; investment decisions for information technologies or systems; monitoring strategies and ongoing authorizations of information systems and common controls. The results of a Tier 2 risk assessment may support decisions affecting, for example: security architecture design decisions; the development of risk-aware mission/business processes; the interpretation of information security policies with respect to organizational information systems and environments in which those systems operate. Finally, the results of a Tier 3 risk assessment may support decisions affecting, for example: design decisions; implementation decisions; operational decisions.

As illustrated in Figure 21, the risk assessment process is composed of four steps: (1) prepare for the assessment, (2) conduct the assessment, (3) communicate the assessment results, and (3) maintain the assessment.

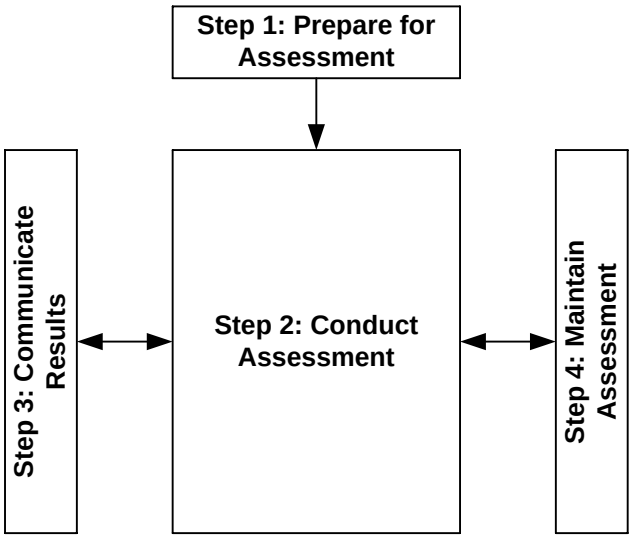

Figure 21: Risk Assessment Process (adapted from NIST 800-30)

The objective of Step 1 is to establish a context for the risk assessment. The establishment of the context depends on the output generated by the risk framing step, which is the first step in the Risk Management Process documented in NIST 800-39 (Managing Information Security Risk – Organization, Mission, and Information System View). NIST 800-30 points out that organizations should carry out the risk framing step to the extent practicable to obtain information to prepare for the risk assessment. Step 1 is initiated based on the outputs of the risk framing step, and consists of the following five sub-steps as given by NIST 800-30.

- Identify the purpose of the assessment.
- Identify the scope of the assessment.
- Identify the assumptions and constraints associated with the assessment.
- Identify the sources of information to be used as inputs to the assessment.
- Identify the risk model and analytic approaches (i.e., assessment and analysis approaches) to be employed during the assessment.

The objective of Step 2 is to conduct the risk assessment and identify a set of security risks that can be prioritized by risk level and used as a basis to support decisions mitigating the risks. Step 2 consists of the following six sub-steps as given by NIST 800-30.

- Identify threat sources that are relevant to the organization.
- Identify threat events that could be produced by those sources.
- Identify vulnerabilities within the organization that could be exploited by threat sources through specific threat events and the predisposing conditions that could affect successful exploitation.
- Determine the likelihood that the identified threat sources would initiate specific threat events and the likelihood that the threat events would be successful.
- Determine the adverse impacts to organizational operations and assets, individuals, other organizations, and the Nation resulting from the exploitation of vulnerabilities by threat sources (through specific threat events).
- Determine information security risks as a combination of likelihood of threat exploitation of vulnerabilities and the impact of such exploitation, including any uncertainties associated with the risk determinations.

Notice that some of the above points use the term "organization" instead of "information system". This reflects one of the main objectives of NIST 800-30, which is to support risk assessment not only at the level of information systems, but also at the organizational level and mission/business processes level. The objective of Step 3 is to communicate and share the risk-assessment results with decision makers across the organization. Step 3 consists of the following two sub-steps as given by NIST 800-30.

- Communicate the risk assessment results.
- Share information developed in the execution of the risk assessment, to support other risk management activities.

The rationale behind the second sub-step above is that the results of a security risk assessment are also useful to other risk management activities that are not related to security. For example, the results of a security risk assessment may support assessments related to cost and performance risks. The objective of Step 4 is to maintain the risk-related information obtained as a result of risk assessment and keep it up to date. This is carried out in order to obtain a risk picture that is up to date, and in order to monitor changes in the risk picture over time. Step 4 consists of the following two sub-steps as given by NIST 800-30.

- Monitor risk factors identified in risk assessments on an ongoing basis and understanding subsequent changes to those factors.
- Update the components of risk assessments reflecting the monitoring activities carried out by organizations.

5.10 NIST 800-37 – guide for applying the risk management framework to federal information systems

NIST 800-37 provides a risk management framework in terms of a structured process consisting of six steps. NIST 800-37 explains the process at a high-level of abstraction and for each step refers to a specific NIST standard in which the step is explained in detail. The purpose of the risk management framework is to:

- Ensure a consistent management of system-related security risks and that this is managed with respect to the organization's mission/business objectives and overall risk strategy.
- Ensure that security requirements and security controls are thightly integrated with the organization's enterprise architecture and system development life cycle process.
- Support consistent, well-informed, and ongoing security authorization decisions through continuous monitoring.
- Achieve more secure information and information systems through appropriate risk mitigation strategies.

As illustrated in Figure 22, the framework consists of the following steps: (1) categorize information system, (2) select security controls, (3) implement security controls, (4) assess security controls, (5) authorize information system, and (6) monitor security controls. According to NIST 800-37, the purpose of these steps is as follows.

- The purpose of Step 1 is to categorize the information system and the information processed, stored, and transmitted by the system based on an impact analysis. The framework refers to NIST 800-60 for a detailed description of this step.
- The purpose of Step 2 is to select an initial set of baseline security controls for the information system based on the security categorization, and then tailoring and supplementing the security control as needed with respect to an organizational risk assessment. The framework refers to NIST 800-53 for a detailed description of this step.
- The purpose of Step 3 is to implement the security controls. The framework refers to NIST 800-160 for a detailed description of this step.
- The purpose of Step 4 is to assess the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly and operating as intended. The framework refers to NIST 800-53A for a detailed description of this step.
- The purpose of Step 5 is to authorize information system operation based on a determination of the severity of risk. This step is explained in detail in NIST 800-37.
- The purpose of Step 6 is to monitor the security controls in the information system on an ongoing basis including assessing control effectiveness (supported by NIST 800-53A), report findings, and conduct security impact analyses of suggested changes.

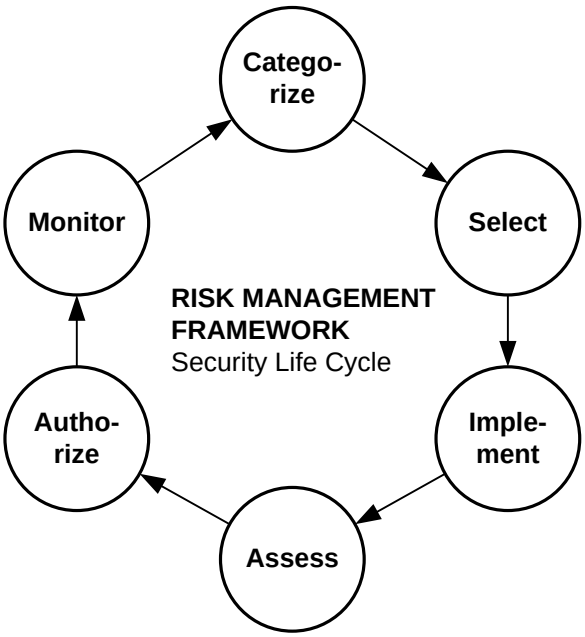

Figure 22: Risk Management Framework (adapted from NIST 800-37)

5.11 NIST 800-53 – security and privacy controls for federal information systems and organizations

The NIST standard Security and Privacy Controls for Federal Information Systems and Organizations (NIST 800-53) provides guidelines for selecting and specifying security controls for organizations and information systems. The guidelines are a part of the NIST Risk Management Framework (NIST 800-37). The guidelines are supported by a process consisting of four steps: selecting security control baselines (Step 1), tailoring baseline security controls (Step 2), documenting the security control selection process (Step 3), and applying the control selection process to new development and legacy systems (Step 4).

Step 1 depends on the output generated by the security categorization step, which is the first step in the Risk Management Framework. The complete security categorization step is documented in NIST 800-60. The purpose of the security categorization step is to determine the criticality and sensitivity of the information to be processed, stored, or transmitted by the information system under analysis. The security category of an information system is expressed in terms of low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability. The generalized format for expressing the security category (SC) of an information system is defined as follows.

$\mathbf{SC}_{\text{information system}}$ = {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)}, where the acceptable values for potential impact are low, moderate, or high.

The above security categorization is carried out for each type of information processed, stored, or transmitted by the information system. Each security category is then mapped to a comprehensive table provided by NIST 800-53 in order to select an appropriate security control baseline. The baseline acts as an initial selection of controls.

Having selected appropriate security control baselines, the tailoring process (Step 2) is initiated. The objective of the tailoring process is to modify and align the controls more closely with respect to specific conditions within the organization and the underlying information systems. For example, supplementing the baselines with additional security controls, and providing additional specification information for implementing the controls. According to NIST 800-53, the tailoring process is part of a comprehensive organizational risk management process – framing, assessing, responding to, and

monitoring information security risk. The tailoring process is therefore used to achieve cost-effective, risk-based security that supports organizational mission/business needs.

NIST 800-53 emphasize the importance of documenting the selected set of security controls and the rationale supporting the selection (Step 3). This is important in order to understand the assumptions, constraints, and rationale supporting the risk-based decisions, especially when information systems or environments of operation change, and the risk decisions are revised. The documentation is carried out throughout the complete process of selecting and specifying security controls.

Depending on whether the security controls are to be implemented in a new development, or in a legacy system, the selection process may be carried out from two different perspectives (Step 4). In the former, the security control selection process is applied from a requirements definition perspective, while in the latter it is applied from a gap analysis perspective. NIST 800-53 provides guidelines for each perspective.

5.12 NIST 800-137 – information security continuous monitoring (ISCM) for federal information systems and organizations

NIST 800-137 provides guidelines to assist organizations in the development and implementation of an information security continuous monitoring (ISCM) strategy that provides awareness of threats and vulnerabilities, visibility into organizational assets, and the effectiveness of implemented security controls. All security controls, including common and hybrid controls implemented at the system level, are assessed for effectiveness in accordance with the system security plan and the methods described in NIST 800-53A. The ISCM strategy aims to assure that the security controls are aligned with organizational risk tolerance, as well as to provide information about the current risk picture in order to support response to risks in a timely manner. NIST 800-137 also points out the importance of automation in the context of an ISCM strategy, and provides guidelines for what to consider when selecting or implementing tools to support the ISCM strategy.

Figure 23 shows the process provided by NIST 800-137 to define and implement an ISCM strategy. The process consists of six steps: (1) define, (2) establish, (3) implement, (4) analyse and report, (5) respond, (6) review and update.

According to NIST 800-137, the purpose of the steps is as follows.

- The purpose of Step 1 is to define an ISCM strategy based on risk tolerance that maintains clear visibility into assets, awareness of vulnerabilities, up-to-date threat information, and mission/business impacts.
- The purpose of Step 2 is to establish an ISCM program determining metrics, status monitoring frequencies, control assessment frequencies, and an ISCM technical architecture.
- The purpose of Step 3 is to implement an ISCM program and collect the security-related information required for metrics, assessments, and reporting. Automate collection, analysis, and reporting of data where possible.
- The purpose of Step 4 is to analyse the data collected and report findings, determining the appropriate response.
- The purpose of Step 5 is to respond to findings with technical, management, and operational mitigating activities or acceptance, transference/sharing, or avoidance/rejection.
- The purpose of Step 6 is to review and update the monitoring program, adjusting the ISCM strategy and maturing measurement capabilities to increase visibility into assets and awareness of vulnerabilities.

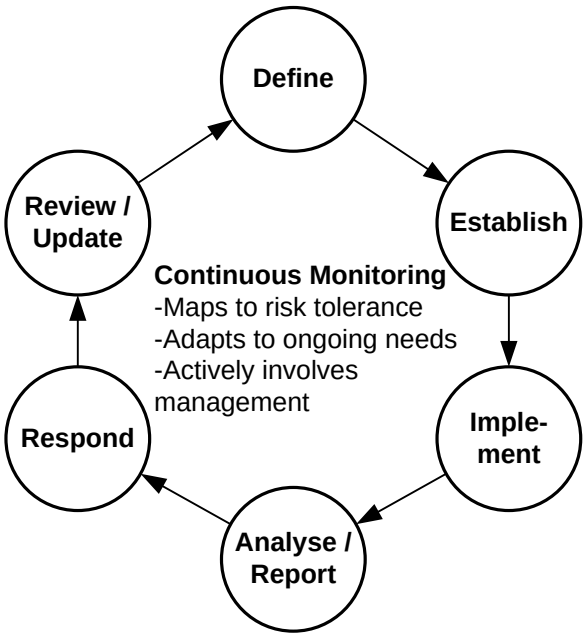

Figure 23: Information Security Continuous Monitoring Process (adapted from NIST 800-137)

Continuous monitoring lies at the centre of the strategy in order to obtain current risk picture and map it to the organizational risk tolerance, adapt to ongoing needs, and actively involve management.

5.13 SANS Institute annual top 20 internet security vulnerability list

The SANS Institute was established in 1989 as a cooperative research and education organization [27]. SANS is one of the largest sources for information security training and security certification in the world, and has an active effort to collect and document success stories, in terms of case studies, in cybersecurity. This SANS-effort is referred to as "SANS What Works in Internet Security".

Based on evidence collected from case studies, SANS reports effective security controls. In particular, SANS has developed a top 20 internet security vulnerability list [27], and provides security controls for each of the vulnerabilities in the list. The security controls SANS provide are a subset of the comprehensive catalogue defined by NIST 800-53, as well as the NIST Framework for Improving Critical Infrastructure Cybersecurity. Thus, the controls provided by SANS do not attempt to replace the work of NIST, but instead prioritize and focus on a smaller number of actionable controls with high-payoff. The following list current critical security controls suggested by SANS. The SANS webpage provides guidelines for how to implement these controls.

1. Inventory of Authorized and Unauthorized Devices.
2. Inventory of Authorized and Unauthorized Software.
3. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers.
4. Continuous Vulnerability Assessment and Remediation.
5. Malware Defences.
6. Application Software Security.
7. Wireless Access Control.
8. Data Recovery Capability.
9. Security Skills Assessment and Appropriate Training to Fill Gaps.

10. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches.
11. Limitation and Control of Network Ports, Protocols, and Services.
12. Controlled Use of Administrative Privileges.
13. Boundary Defence.
14. Maintenance, Monitoring, and Analysis of Audit Logs.
15. Controlled Access Based on the Need to Know.
16. Account Monitoring and Control.
17. Data Protection.
18. Incident Response and Management.
19. Secure Network Engineering.
20. Penetration Tests and Red Team Exercises.

5.14 Cyber Essentials Scheme

The UK Government has developed guidelines, in terms of requirements, supporting organizations in mitigating the most common Internet based threats to cyber security [28]. The main objective is to make the UK a safer place to conduct business online. The Cyber Essentials Scheme acts as supporting material for the Information Risk Management Regime also developed by the UK Government. The Information Risk Management Regime is a 10-step process to: establish an effective governance structure and determine risk appetite, produce supporting information risk management policies, and maintain the stakeholder's engagement with cyber risk.

The Cyber Essentials Scheme was developed together with industry partners such as the Information Security Forum (ISF), the Information Assurance for Small and Medium Enterprises Consortium (IASME), and the British Standards Institution (BSI). According to the Cyber Essential Scheme, the most common cyber attacks organizations are exposed to may be mitigated by implementing security control within the following five main categories.

- Boundary firewalls and internet gateways.
- Secure configuration.
- Access control.
- Malware protection.
- Patch management.

The Cyber Essentials Scheme explains the basic requirements for the above security controls, but refers to ISO 27001 and ISO 27002, as well as ISF and IASME for further guidance.

5.15 Operational Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)

OCTAVE is a method to evaluate information security risks [29]. The method is designed to be led by an interdisciplinary team within an organization, that is, the analysis team. The method is asset driven in the sense that it requires the analysis team to identify information-related assets that are important to the organization, and focus risk analysis activities on the assets perceived as the most critical. In OCTAVE, the analysis team is required to consider the relationships among critical assets, the threats to those assets, and vulnerabilities that may be exploited by threats to harm the assets.

OCTAVE consists of three main phases: (1) build asset-based threat profiles, (2) identify infrastructure vulnerabilities, and (3) develop security strategy and plans. The purpose of Phase 1 is to identify important information-related assets at the organizational level by actively involving staff members, and to identify what is currently being done to protect those assets (security controls).

Then, the analysis team selects the most critical assets by analysing the gathered information. Finally, the team describes security requirements for the critical assets, and identifies potential threats for those assets.

The purpose of Phase 2 is to identify information technology systems and components related to each critical asset. Then, the analysis team identifies vulnerabilities that may be exploited by threats which may in turn harm the assets.

The purpose of Phase 3 is to identify security risks the information system under analysis is exposed to, with respect to the identified assets, threats, and vulnerabilities. Having identified security risks to critical assets, the analysis team creates mitigation plans to address the risks.

OCTAVE underlines that the above method is part of an overall risk management process consisting of six iterative steps: identify, analyse, plan, implement, monitor, and control security risks. The OCTAVE method comprises the steps related to identify, analyse, and plan. OCTAVE points out that these six steps/activities are nothing more than a plan-do-check-act cycle. This is similar to the ISMS process depicted in Figure 16.

5.16 CCTA Risk Analysis and Management Methodology (CRAMM)

The CCTA[3] Risk Analysis and Management Methodology (CRAMM) is based on the UK Government's Risk Analysis and Management Method [30]. CRAMM carries out risk analysis in order to identify security related risks, while risk treatments are identified as part of the risk management process. As illustrated in Figure 24, the method may be divided into two main phases: risk analysis and risk management.

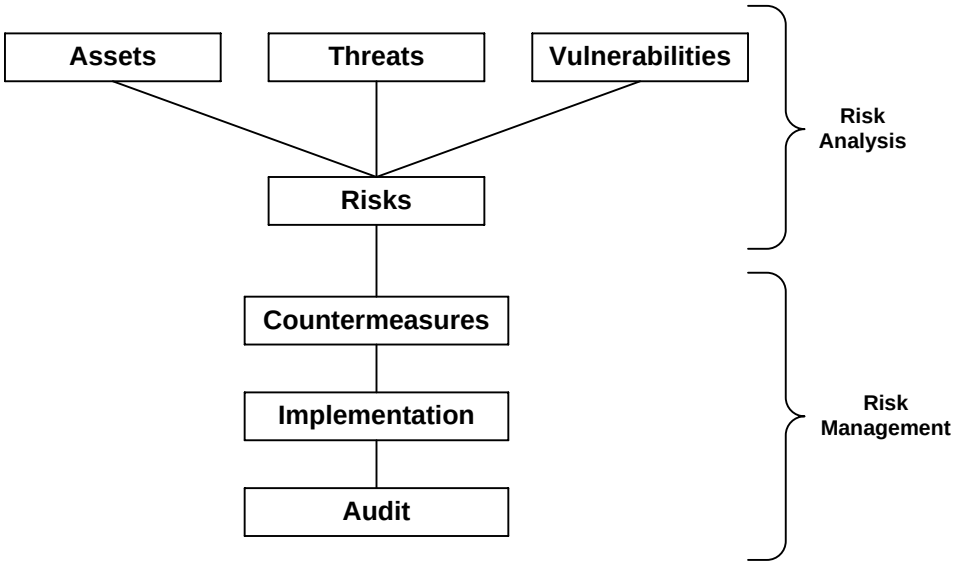

Figure 24: CCTA Risk Analysis and Management Methodology

Risk analysis has three phases dedicated to asset, threat and vulnerability identification. The aim is to identify critical assets, and then threats that may exploit vulnerabilities in order to harm assets, which in turn represent risks. In the risk management phase, countermeasures are identified and implemented. The aim of risk management is to identify requirements for specific controls, demonstrate compliance with standards such as BS 7799, ISO 27001, and ISO 27002, develop business continuity strategy and security policies, and audit the effectiveness of existing security controls.

[3] Central Computer and Telecommunications Agency, now renamed into Office of Government Commerce (OGC), of the United Kingdom government.

CRAMM does not only provide a method as described above, but contains also: a database consisting of over 3500 security controls, a set of tools supporting in achieving certification or compliance against above mentioned standards, useful templates for security documentation, pre-defined risk assessments covering generic information systems, and a set of risk management tools to support security improvement and budget planning.

5.17 CORAS

CORAS [31] is a model-driven approach to security risk analysis, and consists of three artefacts: a language, a tool, and a method. The CORAS approach is based on the ISO 31000 standard on risk management, and is also an asset-driven approach (similar to OCTAVE).

The CORAS language is a customized diagrammatic language for risk modelling, and uses simple graphical symbols and relations to construct diagrams representing the risk picture. The CORAS approach is supposed to be conducted by an interdisciplinary risk analysis team, and the CORAS language supports the construction of risk models that are suitable as a means for communication between stakeholders of diverse backgrounds. The CORAS tool is a graphical editor for making any kind of CORAS diagrams. The tool may be used to create risk models on-the-fly during brainstorming sessions, and also facilitates the documentation and presentation of risk analysis results. The CORAS method is a method for asset-driven risk analysis and is supported by the CORAS language, as well as the CORAS tool. The method consists of eight steps.

- CORAS Step 1, preparation for the analysis, aims to make the necessary preparations for the actual analysis tasks based on a basic understanding of the target.
- CORAS Step 2, customer presentation of the target, aims to get the representatives of the customer to present their overall goals of the analysis, the target they wish to have analysed, and the focus and scope of the analysis.
- CORAS Step 3, refining the target description using asset diagrams, aims to ensure a common understanding of the target of analysis by having the analysis team present their understanding of the target, including its focus, scope and main assets.
- CORAS Step 4, approval of target description, aims to ensure that the background documentation for the rest of the analysis, including the target, focus and scope is correct and complete as seen by the customer.
- CORAS Step 5, risk identification using threat diagrams, aims to systematically identify threats, unwanted incidents, threat scenarios and vulnerabilities with respect to the identified assets.
- CORAS Step 6, risk estimation using threat diagrams, aims to determine the risk level of the risks that are represented by the identified unwanted incidents (discovered in CORAS step 5).
- CORAS Step 7, risk evaluation using risk diagrams, aims to clarify which of the identified risks are acceptable, and which of the risks must be further evaluated for possible treatment.
- CORAS Step 8, risk treatment using treatment diagrams, aims to identify and analyse possible treatments for the unwanted incidents that have emerged. Treatments are assessed with respect to their cost-benefit evaluation, before a final treatment plan is made.

6 Best practice: Security testing

The business planning and execution focuses on making things that work fast and reliable to sufficiently fulfill user's requirements. The security of these processes is frequently on second place, because it is hidden somewhere in the politics of the processes or source code. Users have to trust the service, application and the provider that they care with the data appropriately. Underestimating the importance of the security can lead to data leakage, losing user trust and costs that might get higher than the business can survive.

Creating secure software or business workflows starts with finding its vulnerabilities, when developers and business planers take a role of a “black hat” and critically assess their work on each step and process in business workflow. The WISER project follows the incremental model of security assessment, starting with external testing of vulnerabilities, then progressing with detailed internal monitoring and finally with creating the business mitigation plans and cost benefit calculations. The reader is referred to Section 3 of D2.1 for further explanation of the WISER Risk Management Framework. The similar incremental progress will be used in choosing the tools for making the risk assessment. In this section we provide a few representative examples of tools that can help to assess the business applications from the cybersecurity aspect. These include exploitation databases, Web Application Vulnerability scanners and tool packs frequently used for security testing.

6.1 Security exploits database

Before penetration testing and exploit identification process begins, we need to learn and understand how the vulnerabilities are found and the attacks are planned and executed. First step is to investigate already known exploits and reading security articles.

People and programs leave valuable and vulnerable information on the Internet. If the data is not properly secured, it could be accumulated with search engines or other crawlers that scan the network. Google hacking database, maintained by Offensive Security, is a good entry point to search for fresh security exploits and possible risks. The exploits are documented, descripted and user can even search for them through the Google search engine. The vulnerable applications are on the reach of the click on the Google results pages, until the application owners fix the problem. Fresh exploits are usually quite new and not yet integrated in the tools presented in the rest of the section. Beside the exploits the database includes a list of security papers and articles from all over the world.

6.2 Web application Scanners

Web Application Vulnerability Scanners are automated tools that scan web applications to look for known security vulnerabilities such as cross-site scripting, SQL injection, command execution, directory traversal and insecure server configuration. A large number of both commercial and open source tools are available and all these tools have their own strengths and weaknesses. OWASP provides a good overview over available tools [47].In the following we present some of these in order to illustrate capabilities typically offered by such tools.

6.3 Grabber

Grabber 4is an open-source web application scanner provided by Romain Gaucher. It is a small tool without GUI and is designed for small web pages due to its low speed. The main advantage of the tool is on Blind SQL Injection, SQL Injection and File Inclusion. Grabber provides also an additional module named Crystal that allows combination of source code scanning and application scanning.

6.4 Vega

Vega[5] is free and open source web application scanner provided by Subgraph in Montreal. The focus of the Vega application is on cross-site scripting (XSS) and SQL injection. Vega includes an automated scanner for quick tests and an intercepting proxy for tactical inspection.

6.5 Owasp ZAP

OWASP ZAP is free and one of the most active OWASP projects developed by international team of volunteers. ZAP is a short name for Zed Attach Proxy, which is an open-source integrated penetration

[4] http://rgaucher.info/beta/grabber/
[5] https://subgraph.com/vega/

testing tool based on Java. It is cross platform and internationalized in many languages and has comprehensive help pages.

The ZAP main features are:

- Intercepting Proxy Active and Passive Scanners (proxying browser's requests through the proxy server).
- Passive and Active scanning (passive scanner examines requests and responses, safe for use on any web page. Active scanners are bit more advanced and can change the content of the requests, can issue an attack).
- Spider (crawling, traversing web resources on the page being scanned).
- Report Generation (reports on found issues with links on more details, mitigation process).
- Brute Force (using OWASP DirBuster code, finding files hosted on the web server with no links towards the files).
- Fuzzing (using OWASP JBroFuzz code, completes automated scanners with more sophisticated input request generation process).
- Auto tagging (tagging messages, detecting which web pages have hidden fields).
- Port scanner (detecting opened ports of the applications).
- Smart card support (assessment of the token authentication process).
- Session comparison
- Invoke external apps
- BeanShell integration
- API + Headless mode
- Dynamic SSL Certificates
- Anti CSRF token handling

6.6 W3af

The w3af[6] project's goal is to create a framework to help you secure your web applications by finding and exploiting all web application vulnerabilities. The application provides GUI and preconfigured templates for executing penetration tests.

6.7 Acunetix Web Vulnerability Scanner (WVS)

Acunetix Web Vulnerability Scanner [32] is a commercial Web application security testing tool. It can be used to audit a Web application by checking for vulnerabilities such as SQL injection, cross site scripting and other exploitable vulnerabilities. Additionally, it offers a solution for analysing off-the-shelf and custom Web applications [33]. It also allows testers to create user defined vulnerability tests that can be added to the existing library of vulnerability tests in the tool. The tool also allows users to create customized scan profiles in order to perform specific security tests and thereby reduce the total scan time. The following six points briefly explain how automated security scanning in Acunetix WVS works:

1. The crawler scans the entire website by following all the links on the site. Then it displays a tree structure of the website and detailed information of each discovered file.
2. After the crawling process, Acunetix WVS launches vulnerability attacks on each page found, and thereby emulating a hacker.

[6] http://w3af.org/

3. If the port scanner option is enabled, Acunetix WVS will perform network security checks against the services running on the open ports.
4. Acunetix WVS displays each vulnerability as they are detected and places them under an alert node. Alert nodes can either be high, medium or low. It is further possible to look closer into one vulnerability and find information like the HTTP response, the source code line and its vulnerable part, stack trace etc. For each discovered vulnerability, Acunetix WVS gives a recommendation on how to fix it.
5. Open ports will be listed along with the security tests that were performed.
6. Finally, it is possible to save a complete scan for later analysis, comparison, or report generation.

Acunetix WVS provides an array of tools for security testing commonly found in other commercial web vulnerability scanners, such as port scanners, subdomain scanners, SQL and XSS injectors, HTTP sniffers and fuzzers, authentication testers etc. However, the tool puts an extra emphasis on mitigating the number of false positives, commonly produced by web vulnerability scanners, by making use of what is referred to as AcuSensor Technology [33], [46]. The AcuSensor Technology achieves this by combining black-box scanning techniques with dynamic code analyses while the source code is executed. Figure 25 illustrates how the AcuSensor Technology works.

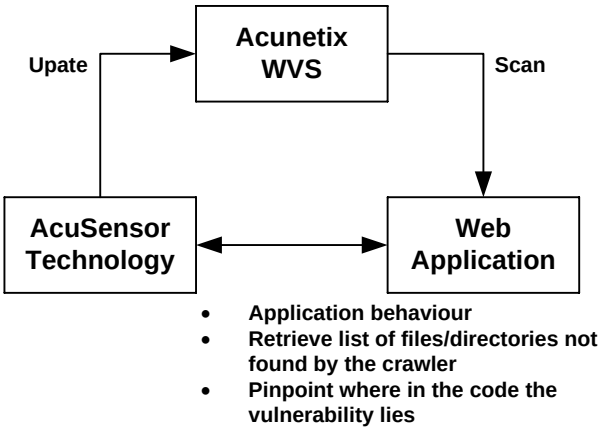

Figure 25: Acunetix AcuSensor (adapted from [46])

6.8 Portswigger Burp Suite

Burp Suite [34] is a free Web application security testing tool. Similar to OWASP ZAP, this tool provides some automatic testing features, as well as a platform that is highly configurable in the sense that users are able to manually implement specific security tests. The features related to manual implementation of tests require advanced testing skills. This tool has many of OWASP ZAP's functionalities, and supports similar automatic security testing features. Burp Suite contains the following key components.

- An intercepting Proxy, which lets you inspect and modify traffic between your browser and the target application.
- An application-aware Spider, for crawling content and functionality.
- An advanced web application Scanner, for automating the detection of numerous types of vulnerability.
- An Intruder tool, for performing powerful customized attacks to find and exploit unusual vulnerabilities.
- A Repeater tool, for manipulating and resending individual requests.

- A Sequencer tool, for testing the randomness of session tokens.
- The ability to save your work and resume working later.
- Extensibility, allowing you to easily write your own plugins, to perform complex and highly customized tasks within Burp.

6.9 N-Stalker Scanner

N-Stalker Scanner is a commercial Web application security testing tool. In addition to scanning for security vulnerabilities in Web applications, it is also built to provide a better control over the Web Application Development Life-cycle [35]. This is done by letting the users create specific security scan policies to cover; (1) development & QA profiles, (2) infrastructure & deployment profiles, and (3) penetration testing and security auditing profiles. This tool has a high level of automated security testing coverage, and has the capability of saving scan results and crawl results separately. N-Stalker contains the following key components.

- Custom Design Errors (cross-site scripting injection, parameter tampering, header splitting, carriage return and line feed (CRLF) injection attacks, etc.).
- Web Server Exposure (web server infrastructure analysis module, SSL encryption vulnerabilities, HTTP Protocol vulnerabilities, etc.).
- Web Signature Attacks supported by a database consisting of 40,000 attacks.
- Confidentiality Exposure Checks (insecure methods for sending data, information leakage, insufficient encryption, etc.).
- Cookie Exposure Checks (weakness in cookie information, information leakage in cookie information, cookies vulnerable to client-side script, etc.).
- File and Directory Exposure Checks (search for backup files, configuration files, password files, etc.).

6.10 IBM Rational AppScan

IBM Rational AppScan [36], [37], is a security vulnerability testing tool for web applications and web services. Similar to N-Stalker Scanner, AppScan lets users create customized scanning profiles in order to get better control over the Web Application Development Life-cycle. This tool has a high level of automated security testing coverage, but does not have the capability of saving scan results and crawl results separately. AppScan may be used in three distinct testing techniques that complement each other: dynamic analysis (black-box scanning), static analysis (white-box scanning), and interactive analysis (glass-box scanning).

AppScan provides a large number of security testing features and is part of the IBM's integrated solution for application security risk management, which also consists of the IBM Security Network Intrusion Prevention System, as well as the IBM InfoSphere Guardium System. The main purpose of the Network Intrusion Prevention System is to monitor network activity and to protect web applications. The main purpose of the InfoSphere Guardium System is to assess database vulnerabilities and monitor database activity [38].

According to the user manual of AppScan version 9.0.0.1 [37], AppScan also provides advanced features supporting general and regulatory compliance reporting, customization and extensibility through a dedicated extendibility framework, and categorization of links in order to identify risks posed to users from links to malicious or other unwanted sites.

6.11 HP WebInspect

HP WebInspect [39] is a commercial Web application security testing tool. WebInspect provides a similar set of features as IBM Rational AppScan. However, WebInspect differs from other similar tools

in the sense that it can perform security tests during the crawling process (simultaneous crawl and audit). Moreover, WebInspect has a high level of automated security testing coverage, and has the capability of saving scan results and crawl results separately. WebInspect and AppScan are, according to Forrester [40], the most advanced and leading commercial application security testing tools.

6.12 Automated Vulnerability Detection System (AVDS)

AVDS is developed by the company Beyond Security, and is a complete network scanning solution used to test the nodes in a network including equipment, applications, and web apps [41]. AVDS is capable of running tests in a network consisting of 50 to 20,000 nodes. A typical execution of AVDS consists of the identification and characterization of network nodes, followed by automatic testing with respect to the characteristics of the node under test. This tool is supported by a database consisting of 10,000 known vulnerabilities, and the database is continuously updated by the tool provider. Moreover, the tool allows organizations to customize risk policies, and manage risks through assets values rather than vulnerability values.

7 Best practice: Vulnerability and threat monitoring

Due to the high complexity of current systems and the fact, that they are based on various technologies, raises the problem of creating potential multiple attack vectors and many weak nodes that might be exploited. Security testing and vulnerability scanning is a preventive best-practice providing defences and securing holes in the system during its design and maintenance. Despite the advanced tools for security testing and rich repositories of vulnerabilities, systems still remain under the threat of an attack or breach. New vulnerabilities, in different technologies, are being discovered on a daily basis and attackers invent more and more clever and stealthy attacks deceiving the users of the system and making them cause unintentional damage.

To combat those sophisticated threats various vulnerability and threat monitoring techniques can be introduced in order to increase the security of the system, detecting and mitigating suspicious activities that might be a sign of an active attack being carried out. The detection mechanisms are usually automated monitoring sensors that are able to perform analyses on a stream of data or classify certain patterns found within the captured data, often in real time.

7.1 ATOS R-LING High performance phishing detection

The R-LING module is aimed at phishing web sites detection based on simple heuristics. It is a machine learning based module that has the capability of stream (real-time) learning and is able to adapt to dynamically changing environments. It is also characterized by high performance and can serve as a pre-filter for high volumes of data. It is built from three main components:

- **Crawler component -** The crawler components is responsible for downloading information from various sources, providing malicious and benign web sites, and builds an internal training dataset for the machine learning component. It activates itself automatically in intervals of time.
- **Learning and analysis component –** It uses the training dataset created by the crawlers and uses it for adjusting the current configuration of the classification mechanism.
- **Communication components -** The Communications components exposes a REST API allowing to submit URLs, of suspicious websites, and provides a classification according to the current state of the system.

7.2 ATOS DNS traffic analysis module

The DNS traffic analysis module looks for certain patterns and features within the DNS traffic and tries to identify patterns that lead to Fast Flux Service Networks (FFSN), and in the end, domains and IP

addresses that could be potentially belong to a botnet used for malicious purposes such as DDoS attacks, malware distribution centers, etc.

The module consists of several components that focus on the analyses of certain features of the DNS data, and produces a list of suspicious domains, IP addresses and a score associated to them. Afterwards, an orchestration component implements an algorithm that takes into account the output score of each of the modules and computes the resulting likelihood associated to the domains and IP addresses. Besides the DNS data, which is the main source for the component, the component also takes as input public available blacklists and whitelists.

7.3 ATOS Netflow traffic analysis module

The analysis of Netflow data aims at identifying botnets by discovering anomalous behavior in the network traffic. These observations may lead, for instance, to identify the hosts in the network that are part of a botnet, but also to the identification of a compromised network device and the C&C server that is sending commands to it.

The analysis module is receiving as input the Netflow data generated by the communication node which might be a switch or a router that is mediating the incoming/outgoing traffic between the systems internal hosts and the Internet. The Netflow data is processed by the Netflow Behavior Analysis Module to detect anomalous behavior that may lead to a conclusion that the systems infrastructure is being used by a C&C server and that the network device has been compromised. Besides the analysis of the network behavior represented by the Netflow captured data, the sensor takes a list of domains, IP addresses and DNS servers, as input, that are known to be malicious in order to identify connections to C&C servers, malicious web servers for malware distribution or to detect DNS spoofing.

7.4 SNORT

Snort is an intrusion detection system available under a free license. It consists of a wide range of mechanisms for attack detection and enables, in real time, the analysis of traffic and packet going through the network based on the IP/TCP/UDP/ICMP protocols. In is capable of conducting packet stream analysis and searching for suspicious content as well as detecting various kinds of attacks and anomalies, such as buffer overflow, port scanning, attacks on WWW web pages, attempts of detecting the operating system and many more. SNORT can function as an independent sniffer, an intrusion detection system or intrusion prevention system.

7.5 AIDE (Advanced Intrusion Detection Environment)

AIDE is a system that stores a snapshot of the systems state, modification times and other configuration information specified by the administrator. The administrator is then able to perform integrity tests against the snapshot and the real sate of the system taken later on. If there are any inconsistencies AIDE will detect them and produce a report.

7.6 Suricata

Suricata is a IDS, IDP and Network Security Monitoring engine. It is an open source tool owned by a community and run by a non-profit foundation, the Open Information Security Foundation (OISF). It is highly scalable and can take full advantage of multiprocessor hardware systems allowing achieving very high performance and real time analysis on live traffic.

Most common protocols are automatically recognized allowing writing rules concerning protocols themselfs and not assigning rules to particular ports, where the protocol is expected. Additionally Suricata implements dedicated keywords that can be matched with protocol fields which range from http URI to a SSL certificate identifier.

Suricata is also capable of identifying files being transferred within the network by calculating MD5 checksums on the fly and comparing them with a list of md5 hashes of restricted files.

7.7 Tenable Nessus

Nessus is developed by Tenable Network Security and is a vulnerability scanner providing features related to vulnerability detection, scanning, and auditing [42]. The features provided by Nessus may be grouped into three categories: reporting and monitoring, scanning capabilities, and deployment and management. The following points list the overall scanning capabilities of Nessus [43].

- Asset discovery
- Vulnerability scanning
- Broad asset coverage and profiling including network devices, operating systems, databases, web applications, cloud applications, and compliance verification
- Threat auditing for detecting viruses, malware, backdoors, hosts communicating with botnet-infected systems, etc.
- Control Systems Auditing including SCADA systems and embedded devices
- Sensitive Content Auditing such as credit card numbers

Nessus is also provided as software as a service (SaaS), maintained and operated by Tenable Network Security.

7.8 IKare

IKare is a fully automated monitoring tool similar to Nessus for security and vulnerability assessment [44]. IKare is a light scanner that that provides real time monitoring by introducing a notion of "memory" between two scans [44]. Similar to Nessus, IKare may also be provided as SaaS allowing users to scan globally with no additional infrastructure. IKare includes the following features.

- Asset discovery: Assets are automatically discovered through the IKare scanner which discovers devices and applications such as firewalls, servers, operating systems, wireless devices, etc.
- Security monitoring: Systems are scanned to check if they comply with security "best practices" based on a vulnerability knowledge base.
- Vulnerability management: IKare detects vulnerabilities across the network as well as vulnerabilities on web applications.
- Analyze threats: IKare's reports provide executive summaries, as well as detailed analysis including all vulnerabilities and risk factors.

8 Conclusions

This report provides a first basis for requirements elicitation and early design of the WISER framework. There are two ways in which the report contributes to achieve this. First, we have established within the consortium an initial shared understanding of the associate partners and their businesses, as well as their current practices, challenges and overall needs with respect to cyber security and risk management. This also represents the first step in the process of developing the early assessment pilots that are conducted for the associate partners. While there is still a lot to learn about the associate partners, the understanding we have established at this early stage provides a highly useful starting point and allowed us to identify some important characteristics for the WISER framework. In particular, it is very clear that the framework needs to offer support at different levels of complexity – including lightweight approaches that do not require extensive resources and highly specialized skills. During the rest of the project, and the first year in particular, we will establish a deeper understanding of each of the associate partners, including more details of their ICT infrastructures and current controls. A final version of this report, D6.2 is due in M12.

Our second contribution to the basis for requirement elicitation and early design is to provide an overview of best practices with respect to cyber security and risk management. Here we have focused on established standards, as well as methods and tools for security testing and vulnerability and threat monitoring that are seen as mature enough to be usable in real-life practical contexts. This has allowed us to better understand what solutions are currently available that we can exploit, learn from or build on.

Together, our current understanding of the businesses, needs and challenges of the associate partners and of the current best practice has helped us identify the initial requirements and design for the WISER framework, which is documented in D2.1. Work on D2.1 and D6.1 has been performed in parallel. The initial requirements and design will be further refined based on the continuing work on the EAPs during the first year of the project.

9 References

[1] *Portic mission* (Portic official website) : http://www.portic.net/ENG/mision.shtml

[2] *Closed set of messages exchanged in the different workflows performing the daily operation of Barcelona port* (Portic official website, in Spanish): http://www.portic.net/doc_usuario/ENG/guias_esmt_index_eng.shtml

[3] *Portic document circuit* (Portic official website, in Spanish)*:* http://www.portic.net/doc_usuario/material_formacion/esmt/CircuitoESMT.pdf

[4] *Containers shipment procedure* (Portic official website, in Spanish)*:* http://www.portic.net/doc_usuario/material_formacion/esmt/traslado_de_contenedores_llenos.pdf

[5] *Contingency plan* (Portic official website, in Spanish): http://content.portdebarcelona.cat/cntmng/d/d/workspace/SpacesStore/3c4863b1-8c6f-41ab-a421-a3146632ca01/PContingenciasESMTv30final.pdf

[6] Port Community System definition: http://www.epcsa.eu/pcs

[7] AENOR: *ISO 9001 para la pequeña empresa* (In Spanish). AENOR ediciones. http://www.aenor.es/aenor/normas/ediciones/fichae.asp?codigo=10686#.VaeD0PntlBc

[8] AENOR: *UNE 158401. Servicios para la promoción de la autonomía personal. Gestión del servicio de teleasistencia. Requisitos* (in Spanish).

[9] Spanish Government: *Magerit methodology*. Manuals. Available for downloading on http://administracionelectronica.gob.es/ctt/magerit/descargas#.VaeFUvntlBc

[10] Nagios official website: http://www.nagios.org

[11] Tunstall Televida corporate website: http://tunstalltelevida.es/tunstalltelevida/

[12] *ISO 9001 Quality Management Systems:* http://www.iso.org/iso/home/standards/management-standards/iso_9000/iso9001_revision.htm

[13] *ISO 14001 Environmental Management Systems*: http://www.iso.org/iso/home/standards/management-standards/iso14000/iso14001_revision.htm

[14] International Organization for Standardization / International Electrotechnical Commission: ISO/IEC 31000 – Risk management – Principles and guidelines (2009)

[15] International Organization for Standardization / International Electrotechnical Commission: ISO/IEC 31010 – Risk management – Risk assessment techniques (2009)

[16] International Organization for Standardization / International Electrotechnical Commission: ISO/IEC 27001 – Information technology – Security techniques – Information security management systems – Requirements (2013)

[17] International Organization for Standardization / International Electrotechnical Commission: ISO/IEC 27005 – Information technology – Security techniques – Information security risk management (2011)

[18] International Organization for Standardization / International Electrotechnical Commission: ISO/IEC 27032 – Information technology – Security techniques – Guidelines for cybersecurity (2005)

[19] National Institute of Standards and Technology: Framework for improving critical infrastructure cybersecurity, v1.0 (2014)

[20] National Institute of Standards and Technology: Managing Information Security Risk – Organization, Mission, and Information System view, special publication 800-39 (2011)

[21] National Institute of Standards and Technology: Guide for Conducting Risk Assessment, special publication 800-30 (2012)

[22] National Institute of Standards and Technology: Guide for Applying Risk Management Framework to Federal Information Systems – A Security Life Cycle Approach, special publication 800-37 (2010)

[23] National Institute of Standards and Technology: Guide for Mapping Types of Information and Information Systems to Security Categories, special publication 800-60 Volume 1 (2008)

[24] National Institute of Standards and Technology: Security and Privacy Controls for Federal Information Systems and Organizations, special publication 800-53 (2013)

[25] National Institute of Standards and Technology: Assessing Security and Privacy Controls in Federal Information Systems and Organizations, special publication 800-53A (2014)

[26] National Institute of Standards and Technology: Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, special publication 800-137 (2011)

[27] The SANS Institute. Critical Security Controls - Version 5. https://www.sans.org/critical-security-controls/ (Accessed: August 2015)

[28] HM Government. Cyber Essentials Scheme – Requirements for basic technical protection from cyber attacks. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317481/Cyber_Essentials_Requirements.pdf (Accessed: August 2015)

[29] Alberts, C.J., Davey, J.: Operational Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) criteria version 2.0. Technical report CMU/SEI-2001-TR-016. Carnegie Mellon University (2004)

[30] Barber, B., Davey, J.: The use of the CCTA risk analysis and management methodology (CRAMM) in health information systems. In: 7th International Congress on Medical Informatics, MEDINFO'92, pp. 1589-1593. North-Holland, Amsterdam (1992)

[31] Lund, M.S., Solhaug, B., Stølen, K.: Model-driven risk analysis – The CORAS approach. Springer (2011)

[32] Acunetix Web Vulnerability Scanner (WVS). http://www.acunetix.com/vulnerability-scanner/ (Accessed: August 2015)

[33] Acunetix Web Vulnerability Scanner v10 Product Manual. http://www.acunetix.com/resources/wvsmanual.pdf (Accessed: August 2015)

[34] Burp Suite. https://portswigger.net/burp/ (Accessed: August 2015)

[35] N-Stalker. http://www.nstalker.com/manual/ (Accessed: August 2015)

[36] IBM Rational AppScan. http://www-03.ibm.com/software/products/en/appscan (Accessed: August 2015)

[37] IBM Security AppScan Standard Version 9.0.0.1 User Guide. http://publibfp.dhe.ibm.com/epubs/pdf/c2766180.pdf (Accessed: August 2015)

[38] IBM Software. Breaking down silos of protection: An integrated approach to managing application security. Thought Leadership White Paper (2013). http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=SA&subtype=WH&htmlfid=WGW03035USEN (Accessed: August 2015)

[39] HP WebInspect. http://www8.hp.com/us/en/software-solutions/webinspect-dynamic-analysis-dast/ (Accessed: August 2015)

[40] Taylor Shields. The Forrester Wave: Application Security, Q4 2014. Forrester. http://www.forrester.com/pimages/rws/reprints/document/109101/oid/1-PBFBZ1 (Accessed: August 2015)

[41] Beyond Security. AVDS Vulnerability Assessment and Management. http://www.beyondsecurity.com/avds.html (Accessed: August 2015)

[42] Tenable Network Security. Nessus Manager. http://www.tenable.com/sites/drupal.dmz.tenablesecurity.com/files/datasheets/NessusManager-DS-7_April_2015.pdf (Accessed: August 2015)

[43] Tenable Network Security. Nessus Professional Vulnerability Scanner. http://www.tenable.com/sites/drupal.dmz.tenablesecurity.com/files/datasheets/Nessus_Professional_DS_v6.4.pdf (Accessed: August 2015)

[44] ITrust IT Security Services. IKare. http://www.itrust.fr/ressources/Datasheet/DatasheetIKare.pdf (Accessed: August 2015)

[45] CryptoLocker. https://en.wikipedia.org/wiki/CryptoLocker (Accessed: September 2015)

[46] Acunetix AcuSensor Technology. http://www.acunetix.com/vulnerability-scanner/acusensor-technology/ (Accessed: September 2015)

[47] OWASP list of Vulnerability Scanning Tools. https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools (Accessed: August 2015)

[48] Cacti. http://www.cacti.net/ (Accessed: September 2015)

[49] Graphite. https://launchpad.net/graphite (Accessed: September 2015)

[50] Nagios. https://www.nagios.org/. (Accessed: September 2015)

Appendix I Questionnaire for collecting information from associate partners

This appendix shows the questionnaire that was used to collect information from the associate partners.

Introduction

This questionnaire is intended to be used as an aid (in addition to physical and/or telco meetings) to collect input from the early assessment pilots (EAP) for report D6.1. This report is due by the end of August 2015 and aims to provide the WISER consortium with an overall understanding of the organization, business processes and cybersecurity needs and practice for each EAP. The following subsections will be included for each EAP in D6.1:

1. Organization and business goals.
2. Critical business process.
3. Cybersecurity needs and current practice.

Hence, we structure the questionnaire accordingly. For each section we give an indication of the expected page count per EAP.

Questions

1. Organization and business goals (0,5 – 1 pages)
    a. What are the main business goals of the organization?
    b. Please provide a short description of the organization, including overall organizational structure as well as key figures such as annual turnover and number of employees.

2. Critical business process (2-4 pages)
    a. Please provide a high-level description of the critical business processes of your organization where cyber security is important, preferably supported by one or more figures. Include also the main actors of the processes where applicable.
    b. Please provide a high-level description of the ICT infrastructure that supports these business processes. Include specific devices/components that are crucial for conducting these processes, as well as outsourced services or other external dependencies. *(Examples include cloud service based processes, data centers & storage outsourced vs insourced, authentication services, in-house or mobile device, back-up facilities, disaster recovery,..)*
    c. To what degree would you say that the critical business processes of your organization depend on the ICT infrastructure operating as expected? Give a qualitative indication based on your own judgment, supported by a short explanation.(*qualitative assessment could be high, medium or low, need of 24/7 services, estimate of costs of 1 hour downtime.)*

3. Cybersecurity needs and current practice (2-4 pages)
    a. What are your organization's most important assets that could potentially be harmed as a result of cyber-incidents? *Note that by assets we mean anything of value to your organization. In the context of cyber-risk, assets will typically be defined in terms of confidentiality, integrity or availability of data or services ie: web platform, database of contacts, ERP, access to external cloud services.*
    b. Please explain your organization's current approach to risk management, if applicable including answering the following:

i. Does the organization have dedicated (and competent) persons in charge of cyber risk/cyber security?
ii. How often is a risk assessment of the cyber-infrastructure supporting the critical business process conducted?
iii. Do you follow any established approach or standard for risk management or assessment? If so, which approach or standard is used?
iv. Is any kind of automated real-time monitoring of the cyber-infrastructure in place to detect attacks or incidents? If so, please give a short description, and explain which parts of the cyber-infrastructure is being monitored.
v. Do you have recovery plans in place in case of damage as a consequence of cyber-attacks?