University of Applied Sciences and Arts Northwestern Switzerland
School of Business

Critical Infrastructure Information Security Model

MASTER THESIS

Author Michael Schlüter

January 31st, 2015

Supervisor Prof. Dr. Petra Maria Asprion

Master of Science in Business Information Systems

Author

Michael Schlüter

[redacted]

Supervisor

Prof. Dr. Petra Maria Asprion

[redacted]

Abstract

Malfunction of critical infrastructures have a serious impact on health, safety, security and economic wellbeing of citizens and have therefore to be supremely protected. Today's cyber threats gain in importance especially for critical infrastructure as they have enormous potential for damage. Critical infrastructures are the backbone of our nation's economy, security and health.

Different instruments are available to address various information security topics. Some regulations exist for parts of critical infrastructure sectors. But there is currently no unique security level of critical infrastructure enterprises.

Goal of this study is to develop a model for critical infrastructures to prevent and mitigate current cyber risks. Gaps in information security for critical infrastructures were disclosed between available instruments and the needs of critical infrastructure providers.

Primary source is based on case study research. Critical infrastructure experts were interviewed to get information about current situations in critical infrastructure enterprises. Books, documentation and journals in the field of information security or critical infrastructure protection are investigated as secondary resources. These sources were used to build a model by prototyping approach, which then was validated by critical infrastructure experts.

Analysis of the case study discloses gaps in the area of awareness, cyber risk management, education, funding, regulation and technology.

The developed "Critical Infrastructure Information Security Model" describes these areas and shows an improved information security model with focus on cyber risks of critical infrastructures.

Acknowledgements

I would like to express my gratitude to my supervisor Prof. Dr. Petra Asprion for the useful comments, remarks and engagement through the learning process of this master thesis.

Also, I like to thank the participants in my survey, Mark Lütz, Andy Mühlheim, Andreas Schneider and Nick Wenger, who have willingly shared their precious time during the process of interviewing and reviewing the prototype of the CIISM.

A special thank goes to Duane Washington who looked closely for English style and grammar and Patrick Bamert for reviewing the final version of the thesis.

I like to thank my family and friends for their understanding when I was often occupied with my master thesis in my spare time and for their encouraging words. Last but by no means least, I want to thank Rebekka who always was there for me.

Table of Contents

1. INTRODUCTION

1.1 Background

Energy supply, financial services as well as traffic systems are, according to the Swiss Federal Council, part of the Critical Infrastructure (CI) in Switzerland and have therefore great influence on the population (FOCP 2014b). Attacks, human failures or malfunctions of CI's can have enormous consequences to affected enterprises as well as to consumers of their services or products (FOCP 2012b). Failures of CI negatively impact industrial production, public services and communications of a whole country (World Economic Forum 2014).

Today's industry control systems (ICS), an integral part of CI's information infrastructure, such as sensors, controller and other electronic transmitters and receivers are more than ever interconnected and especially connected in some way with the Internet (Andress & Winterfeld 2011, p.125). This enables the operators to control the systems from remote networks and to transfer data between these systems through the Internet. This usability feature makes the system vulnerable to external attacks and dependent on other external systems that are not under the control of the enterprise itself.

Sabotage or espionage are current risk scenarios (Lange & Kippels 2009). This growing risk scope was recognized by the Swiss Government and as a result the Federal Office of Civil Protection (FOCP) has defined Switzerland's Strategy for Critical Infrastructure Protection (CIP), which includes several goals to analyse and minimize risks, define dependencies and promote the confidence and information exchange between public authorities and operators of CI's (FOCP 2007). One challenge in this area is the communication and collaboration between the CI sectors (i.e. energy, public safety or public health) and especially between the single enterprises. This goes along with Perkins claim that someone has to take the responsibility to lead and coordinate this section of important facilities (Perkins 2012).

The Swiss Federal Council defines the national strategy and guidelines for CIP explicitly without mandatory regulations for operators of CI's. They provide a guideline to improve the resilience of CI's. It is in the responsibilities of regulatory agencies of each single sector to apply the guideline and monitor the progress (Wenger 2014). Operators of CI's are also known as Critical Infrastructure Enterprises (CIE's).

A focal point by security professionals are cyber risks according to Ernst&Young's "Global Information Security Survey" 2013 (van Kessel & Allan 2013, p.7) and have a top priority for the year 2014. Cyber attacks are seen by 20% of the respondent as a raising threat scenario to disrupt or deface the organization in comparison with the past report period 2012 (van Kessel & Allan 2013, p.10). This corroborates with Stürmer (2013) who stated that Terrorism, Cyber Warfare or Espionage are late-breaking threats and that CI's requires special attention and observation. The reason is that a single fault or attack can led into harm many people in our community and this should be prevented.

Global risk report of the World Economic Forum (2014, p.17) classify cyber attacks as top five risk in 2012 and 2014 in terms of likelihood and break down of critical information infrastructure as top five risk in terms of impact in 2014. These risks are in the same category as well-known worst-case scenarios of water crises, climate change, natural catastrophes or terrorist attacks (see Figure 1).

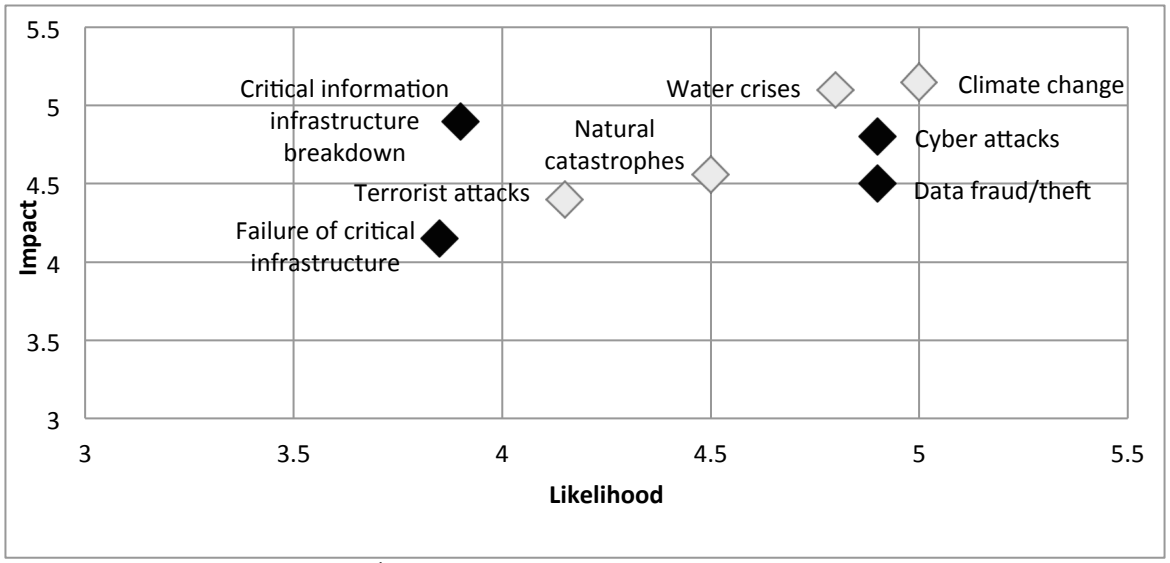

Figure 1: Global Risk Landscape 2014[1] (Simplified from World Economic Forum 2014, p.16)

[1] World Economic Forum Global Risk Report survey respondents were asked to assess the likelihood and impact of the individual risks on a scale of 1 to 7, 1 representing a risk that is not likely to happen or have less impact, and 7 a risk very likely to occur and with massive and devastating impacts (World Economic Forum 2014, p.16)

Cyber risk management differs from traditional risk management approaches where the risk mitigation focus is on risks with high probability and more or less large impact (Barzilay 2013). Cyber risks have the characteristic that they are often classified as improbable – unless they happened recently (Barzilay 2013). "Most of the enterprises reacts the first time when they have been target by an attacker" said Koch, Security Expert of PWC (Barandun 2013). This seems to be the case for cyber risks as the possibility of occurrence is often seen as low but after it's occurrence, the opportunity increases that these risk stays on the risk radar and budget will be allocated to mitigate these risks (Schneider 2014).

CI's are vulnerable and different root causes including cyber attacks can harm them. An example of a nationwide electricity outage of the SBB train network (SBB 2005) in 2005 affected approximately 2000 trains and 200'000 passengers and lead to a financial damage of approximately 5 Mio CHF (VDE 2006). Another power outage in 2008 (NZZ 2008) was triggered by a squirrel that got lost in a power facility of the Elektrizitätswerk der Stadt Zürich (EWZ) in Zürich-Oerlikon caused a short-circuit fault. Amongst others, parts of the CI of the Swiss Broadcasting Corporation (SRG SSR), some public transportation facilities in this area as well around 6000 households were affected. Due to this incidents it is obvious that those exposed infrastructures have to be an essential element of a nations security policy to ensure their protection (Bundesministerium des Innern 2009, p.3).

1.2 Problem Statement

Various CI environments in terms of size, assets and enterprise structure make it difficult to find a generic as well as consistent solution for the inhomogeneous groups of interest. One finding of the literature review is that frameworks with diverse scope and different levels of maturity of information security are available. Different instruments for CIP and cyber security are on the market and used in CIE's. Currently there is no CI sector comprehensive existing regulation or framework. Neither is there a mandatory nor established framework for CIE's based in Switzerland to operate an adequate protection or mitigation especially against cyber risks. For some sub sectors exists different regulations and approaches for CIP i.e. nuclear power stations (Mühlheim 2014). Swiss Federal Councils CIP Guideline addresses all CI's but has no specific focus on cyber risks (Wenger 2014).

Changing attack scenarios of cyber attacks is one of the biggest challenges according to Lütz (2014) and Schneider (2014) remarked, that special designed cyber attacks against an enterprise or individual employee are growing risks. Current frameworks do not focus on cyber risks.

CIE's have to work with already implemented and available instruments; therefore it is necessary to work together with CI experts to fulfil their expectations as well. It's not enough to think on an enterprise- but on a nation-wide risk level. CIE's are not in the position to mitigate all risk deviated from their services as for example Swissgrid (operator of the Swiss electricity transmission system) can't protect all their widespread infrastructure-dependencies by their own (Mühlheim 2014). Are the customers willing to pay for the security or are they prepared to run their business during an outage (Mühlheim 2014)?

1.3 Research Question and Objectives

This research has the aim to improve the situation described in the problem statement with a new or adapted model for CIE's to mitigate cyber risks. The "Critical Infrastructure Information Security Model" (CIISM) should be aligned with the requirements of CIE's in Switzerland.

The research aim is based on the following thesis statement:

> **CIISM addresses current issues with cyber risks for CIE's for the prevention or mitigation of damage through information loss or manipulation.**

Based on the context and purpose of this research, the primary research question is:

> **What are indicators of the CIISM to achieve improvements of the cyber risk prevention or mitigation?**

In order to answer the research question, the following research objectives (RO) can be derived:

- **RO1**: Description of today's cyber risks for CI's
- **RO2**: Observation of used instruments in CIE's to prevent and mitigate CI risks
- **RO3**: Evaluation of current Swiss programs and strategies
- **RO4**: Exploration of discrepancies between existing Swiss programs and strategies and issues of CIE's
- **RO5**: Verification of explored discrepancies with CIE experts

To identify presumed weaknesses of currently used instruments, this research is in addition to the available standards based on secondary sources of expert forums and documentations, as well as currently ongoing and already finished projects of CIP in diverse CI areas of Switzerland. Further important sources are interviews with CI experts; those primary sources are used to get insights in the reality of CIE's.

1.4 Scope and Limitations

CI's are important for almost every economy in all countries and regions worldwide. Switzerland (Bucher et al. 2009) has already started a program to strengthen the protection of CI and as well for example the USA (DHS n.d.) or Switzerland's neighbour Germany (Bundesministerium des Innern 2009) working on strategies to protect their most valuable environment for the population. Internationalization of networks i.e. the energy network, where the national network is connected to the European power network, creates large dependencies on CI's outside of Switzerland (Habegger & Kmiecik 2010, p.6) where other laws and regulations are in place. The scope of the research is limited to CIE's based in Switzerland. But for further usage the CIISM might be adaptable for other countries as well.

CI's have many different risks scenarios but as we live today in the information age the focus is on information security (see definition in section 3.3) and especially on cyber risks.

Many CI sectors includes dozens of CIE´s (FOCP 2014b). For this proposal only a selection of CI experts in high importance sectors are selected and interviewed in the survey to get insights of the reality.

The research proposal was preliminary for the master thesis and handed in on July 31st 2014. The master thesis project started in August 2014 and was finished until end January 2015.

1.5 Research Map

The following research map (Figure 2) visualizes the content of this research paper.

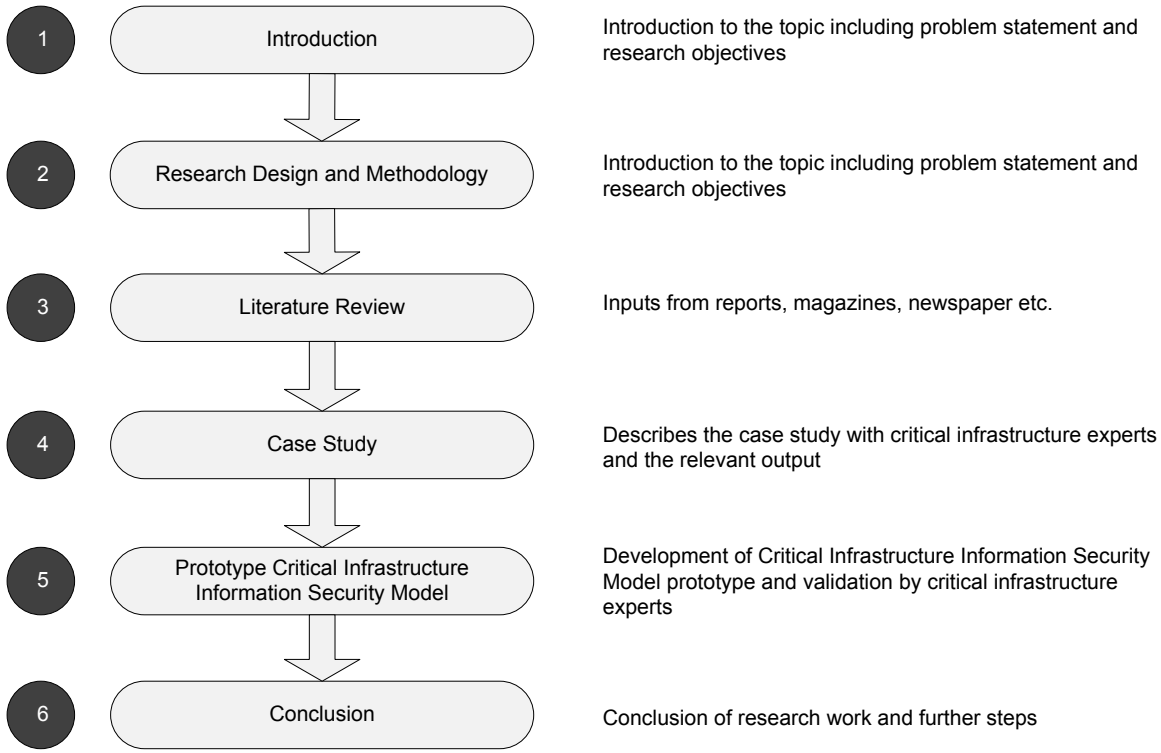

Figure 2: Research Map

2. RESEARCH DESIGN AND METHODOLOGY

The research design is the overall strategy to integrate its different research steps in a systematic and logical order. Saunders et al. (2009) mentioned the research strategy, philosophy, approach as well as the time horizon and the data sources are main components of a research design, which finally are consolidated in the research.

2.1 Strategy

Research strategies are dependent on research questions, their objectives, available sources and the available amount of time to collect the data (Saunders et al. 2009, p.141). Several different types of research strategy methods are mentioned in the literature. Each unit of analysis and its related questions and propositions would call for a (slightly) different research design and data collection strategy (Yin 2009, p.24); therefore a strategy may not use exclusively one method but several combined types.

This research follows a combined strategy of case studies and design science. The case study strategy is used to get insights into a specific environment of CI's where as design science strategy is used to create an artifact combining information gathered from the case study and additional secondary sources. Finally the participants of the case study will validate the created artifact what then will be considered for the revised CIISM version.

The information system research framework by Hevner et al. (2004) in Figure 3 shows how the information system research is strongly related to influences by the Environment and the Knowledge Base.

The relevance of this research is based on the environment and the business needs. Something is relevant for the business if there is a benefit for it. Research is based on input and feedback of interviewed people from the business side to get insights into the culture of CIE's and their technological and organizational issues. Missing appropriate instruments for information security or organizational problems providing an adequate protection for information assets disclose a real business need confirmed by the interviewed CI experts.

Knowledge Base on the right side of Hevner's Research Framework (Figure 3) provides the input to define the CIISM as rigor as possible by use of academic methodologies of design science and theories. Applicable knowledge is important to formalise the vague input from the environment and reach a rigor level.

Research itself includes the main part of Develop/Build the CIISM artifact and the underlying theories. Design science artifacts should be applicable and implementable in practise and therefore the CIISM will be finally assessed by the CIE experts to prove its relevance. The evaluation will then be conducted to finalize a revised CIISM and hand in the research report to the supervisor. (Hevner et al. 2004, p.76)

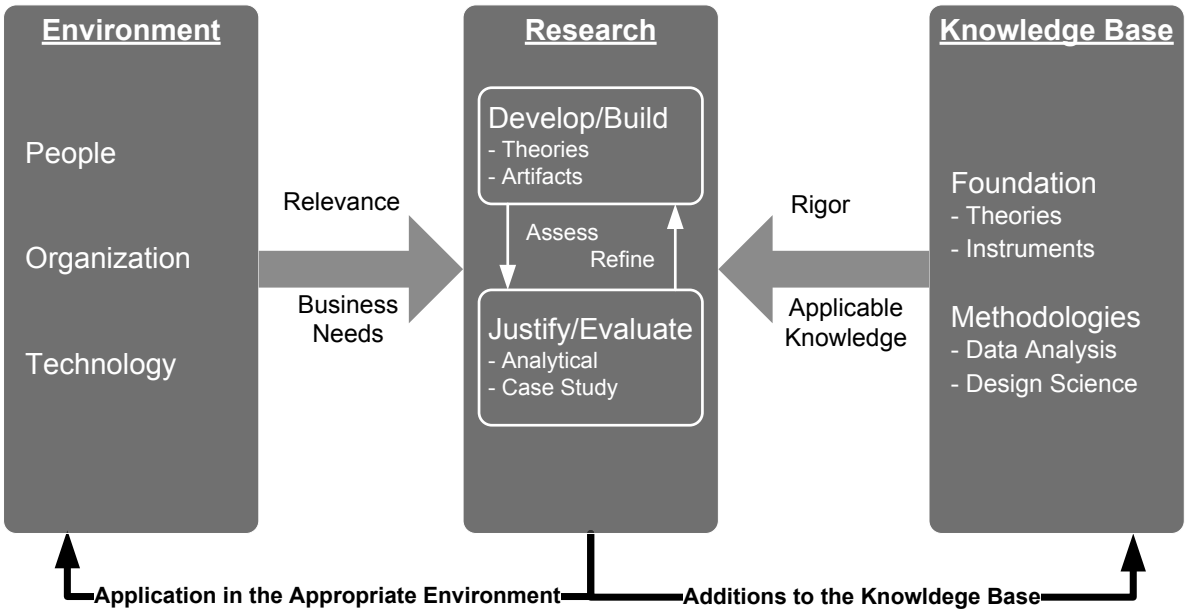

Figure 3: Information System Research Framework (Adopted and simplified; Source: Hevner et al., 2004)

2.1.1 Case Study

Diverse environments with different stakeholders, variable preconditions but common high importance for the population are characteristics of CI's. Small and large, private and public enterprises or low and high regulated markets make it difficult to set common boundaries in this context (see section 10.2). It is the opposition of highly controlled experiment research (Saunders et al. 2009, p.142) where a small but strongly controlled environment is observed.

Case study research is used to get insights into real life situation of CI's dealing with information security and today's cyber risks. Small group of experts give insights of their environment and provide the business need according to Hevner's Information System Research Framework (Figure 3), which then are enhanced with additional secondary sources including mainly literature review.

2.1.2 Design Science

Based on the analysis of the problem findings from the case study design science is used to generate an artifact called CIISM. Design science is fundamentally a problem-solving paradigm where existing knowledge about problems and business requirements are extended with experience, creativity, intuition and problem solving capabilities of the researcher with the intention to build and evaluate problem solving IT artifacts (Hevner et al. 2004, p.76). The newly designed artifact CIISM is specialized on cyber risks for CI's in Switzerland and therefore something new in this area.

2.2 Philosophy

In accordance to Saunders (2009) it doesn't matter if the research paradigm is quantitative or qualitative. Every research is based on underlying assumptions about what is a rigor research and what are the most appropriate research methods.

Positivism philosophy believes in observations and natural science with the goal to verify a new or existing theory with observation or experiment data (Cohen et al. 2007, p.28). Research with positivism philosophy are based on a highly structured methodology to make the result reproducible (Saunders et al. 2009, p.113). Positivism is therefore often used within qualitative research methods and tries to be value free rather than the feeling of the researcher or dependent on instruments (Saunders et al. 2009, p.114). The analyses with positivism philosophy will be expressed in laws or law-like generalizations (Cohen et al. 2007, p.29).

Interpretivism philosophy is different to the positivism philosophy with focus on social actors with the goal to understand the context of complex business environments by involving social actors. An interpretivist interprets social roles with it own set of meanings. Researcher can get access to social actors and phenomena via interviews or survey as well by case study observations (Saunders et al. 2009, p.115).

This research applies mainly on interpretivism philosophy by reason of that the complex situation of different environments and preconditions of CI's cannot be theorized into laws. Therefore the research will be based on inputs of CI experts (social actors) to understand and interpret the different perspective of various CIE's and to evaluate the gaps of existing instruments in the area of information security with focus on cyber risks. Small samples are used to make qualitative in-depth investigations. As the researcher interprets the results, it will be a subjective view with inputs from case studies and therefore the objective approach of positivism philosophy is not applicable. (Saunders et al. 2009, p.119)

Case study analysis supports the philosophy of interpretivism and its applied methodologies by collecting characteristic data of real-life instances with the social actor in focus of observation. It is the aim of this research to investigate selected CIE´s in a real life context. The observations will give first-hand insights about their concerns of information security regarding to cyber risks and the deviated discrepancies of currently used instruments.

Figure 4 visualizes this decision; it shows that qualitative oriented surveys can be based on an interpretivist philosophy according to de Villiers (2005). A qualitative controlled experiment or field experiments could be used in a follow up research applying the generated artifact CIISM derived from the case studies of this research to a large group of CIE's, which is not in scope of this research.

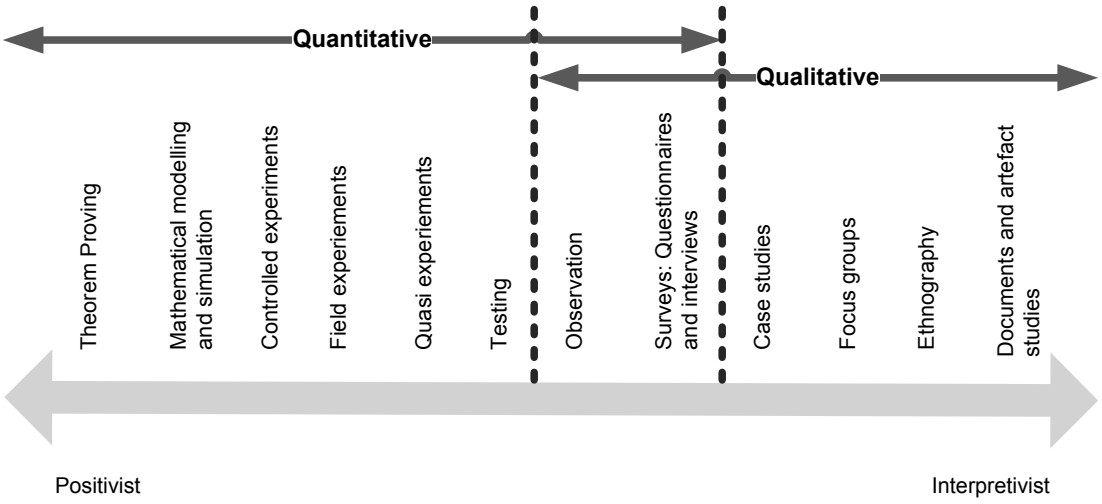

Figure 4: Positivist vs. Interpretivist (Source de Villiers 2005)

2.3 Approach

The research approach describes the method in developing a theory. Inductive and deductive approaches are mentioned in the literature by Saunders et al. and Trochim & Donnelly (2009; 2006). An inductive research approach has the aim to find generalized behaviours from a specific situation, starting with observations or measurements of specific (research) situations to collect (qualitative) data from what common patterns can be derived to formulate a general model. Inductive research is the opposite of deductive research approach with a moving "top-down" procedure form general theory to a hypothesis which will be tested with collected data (Trochim & Donnelly 2006).

This research uses inductive research approach (Figure 5) based on specific observations of situations, which are gained through data collection by literature review of existing ongoing programmes and case studies with experts of CIE's. The outcome of observations discloses common patterns/problems in this field, which lead into a prototype CIISM to improve information security protection with focus on cyber risks. CI experts (social actors) are highly involved into the model design phase creating CIISM, as they should finally benefit from the CIISM or its further development.

Figure 5: Inductive research approach (according to Trochim & Donnelly 2006)

2.4 Time Horizon

The time horizon describes the time period that is observed in the research. Saunders et al. (2009, p.155) describes two ways: the cross-sectional and the longitudinal time horizon.

Longitudinal time horizon includes data of a certain time period. It is often used to investigate the development or change of something. It is also possible to use data of a former research project that can be re-analysed and extend the data set with current data. A longitudinal research time horizon would have been appropriate if focusing on the change of something rather than on a snap shot of time. (Saunders et al. 2009, p.155)

Cross-sectional time horizon is used for this research to investigate a particular situation in a peculiar technological environment. The case study is executed to get insights of a certain snap shot and not investigate on a longer time period (Saunders et al. 2009, p.155). This goes along with the master thesis guidelines to generate and finalize the report between August 2014 and January 2015. Therefore it is not possible to observe changes in the environment over a longer time period.

2.5 Data Sources

This type of research uses a combination of several data collection techniques; interviews during case study and documentary analysis during literature review. (Yin 2009, p.15)

The **primary source** for this research is based on qualitative data retrieved from case study interviews with a selection of CI experts. **Secondary sources** are gathered from literature review basically material from government documentations of the FOCP, the US Department of Homeland Security (DHS) and the German Federal Office for Information Technology as well as referencing literature. This sources are enhanced with books, press releases, professional literature, reports as well documentations of existing instruments and standards.

2.6 Research Model

The research model describes the traceable steps how this report is generated and represents the developed research strategy. The following paragraphs describe in detail the steps (visualized in Figure 6) that are conducted to generate a validated prototype of CIISM based on case study research.

DATA COLLECTION: At the beginning, data is collected with *literature review* method to get an overview about what is common knowledge in the field of research. This includes books, websites, documents and other papers to get an understanding about the meaning of terms like CI's, cyber risks or information security. Also part of this step is the data collection about currently available or ongoing programmes in Switzerland and which instruments and programmes of other countries could be helpful for Swiss CIE's.

CASE STUDY: At this stage, the general terms and knowledge of the data collection based on literature is enhanced with information from *guided interviews* with CI experts. The questions are directed to get information about practices in CIE's to get insights in real life situations. This should disclose what are the used instruments today in CIE's and how are they applied. Further it should give an overview about the expectations of CI experts and how they can be supported with a new or adapted model.

ANALYSES & DIAGNOSIS: In this step, the findings of the interviews and data collection are evaluated. To disclose discrepancies of available instruments and expectations, a gap analysis method is used. Further it should show the difficulties of implementations of (mandatory or best practice) instruments in a CIE and what parts are missing in available instruments from the perspective of CI experts in the field of information security with focus on cyber risks.

PROTOTYPE: The evaluated gaps of the previous step are cornerstones for "Prototype" where a first draft version of the CIISM is developed using design science method. This draft model includes topics and details of a new or adapted model for information security with focus on cyber risks.

VALIDATION: To validate the generated output of the previous step, previously involved CI experts will be asked to verify the prototype of the model during reviews. They are requested to evaluate the prototype and give feedback about feasibility and relevance of the model and its specific elements.

FINAL PROTOTYPE: The validation result flows back into the prototype design and final prototype of the CIISM. The final version includes necessary topics addressing the needs of CI experts and today's cyber risks adequately.

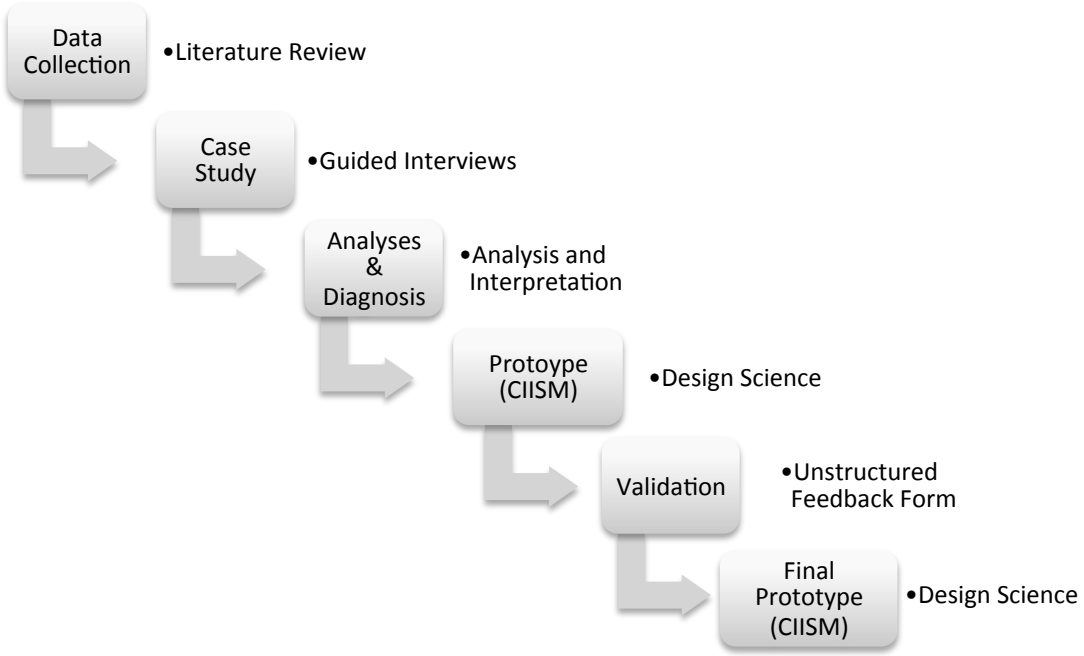

Figure 6: Research Model

3. LITERATURE REVIEW

3.1 Cyber Risks

To understand the term cyber risk it is necessary to start with a traditional risk curve (Figure 7) that correlates the probability of occurrence and its potential impact. A traditional risk management of an enterprise has its risk mitigation focus group on risks with high probability and a more or less large impact, which can be called in this context "Information Security Risks" (Barzilay 2013).

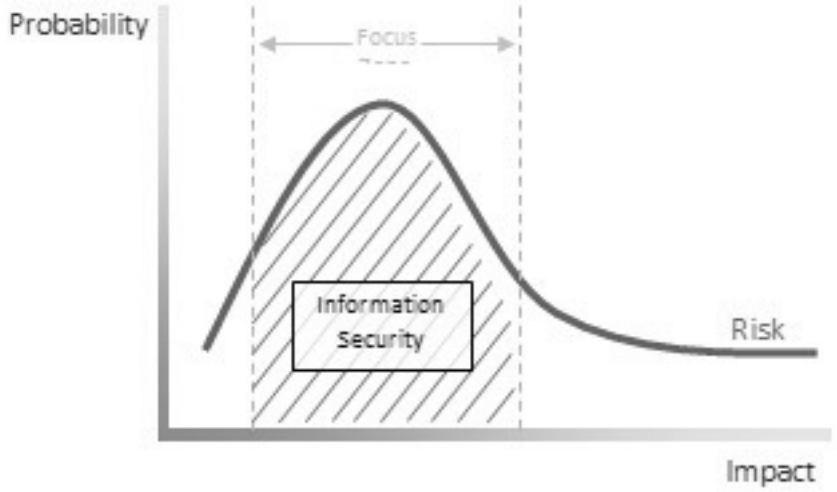

Figure 7: Traditional risk curve with focus group (Source Barzilay 2013)

Cyber risks have the characteristic that they are often classified as improbable – unless they happen recently (Barzilay 2013). New and fast changing cyber risks called advanced persistent threats according to Barzilay (2013); i.e. (1) specially designed malwares, (2) manipulated hardware and firmware, (3) the usage of stolen certifications, (4) spies and informants, (5) exploiting vulnerabilities in archaic hardware or (6) attacking third-party service providers. Focus group of the risk curve (Figure 7) must be adjusted to address the new focus group of very-high-impact risks.

These risks are called cyber security risks and can be very unlikely but possible and can have a high impact. Cyber risks are defined by Barzilay (2013) as part of "Information Security Risks" and therefore the former term "Information Security Risks" is renamed to "Traditional Security Risks" in Figure 8. To avoid a disaster outage or unrecoverable damage of information, these risks should be defined and taken into account.

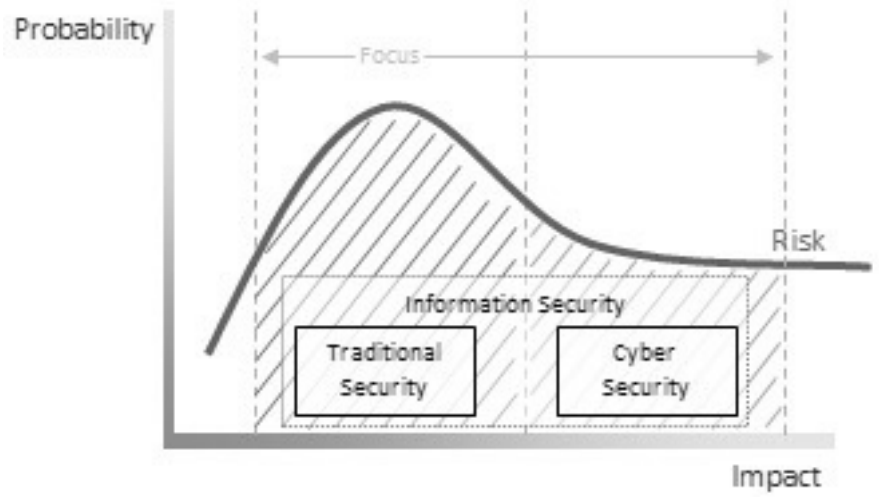

Figure 8: Adjusted risk curve to cyber security risk (Source Barzilay 2013)

"Most of the enterprises reacts the first time when they have been target by an attacker" said Koch, Security Expert PWC (Barandun 2013). This seems to be the case for cyber security risks as the possibility of occurrence is often seen as low but after it's occurrence, the chance increases that these risk stays on the risk radar and budget will be given to mitigate these risk (Schneider 2014).

Changing attack scenarios of cyber attacks is one of the biggest challenges according to Lütz (2014) and special designed cyber attacks against an enterprise or individual employee is a growing risk mentioned Schneider (2014).

3.2 Critical Infrastructures

The Swiss Government determines referenced sectors of CI's in this research. These infrastructures are different to other businesses and have an enormous criticality to the Swiss community. This section is fundamental especially for research objective RO1 (explained in section 1.3). It defines what are CI's and gives a short extract of past cases of disruptions as well a list of current programmes in the area of CI protection.

Several definitions of CI exist and circumscribe CI in different words but with similar meaning. Two definitions are outlined in this section to establish a common understanding of the term. The selection of definitions is chosen by the relevance and size of existing programmes for CIP in the EU and the USA.

Definition: *"Critical infrastructure: an asset, system or part thereof located in Member States that is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact on a Member State as a result of the failure to maintain those functions."* (Europa 2009)

Definition: *"Critical infrastructure is the backbone of our nation's economy, security and health. We know it as the power we use in our homes, the water we drink, the transportation that moves us, and the communication systems we rely on to stay in touch with friends and family. Critical infrastructure are the assets, systems, and networks, whether physical or virtual, so vital […] that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."* (DHS n.d.)

Table 1 lists 10 main sectors with in total 28 sub sectors of CI distinguished by the FOCP (2014b) to get an overview of which businesses have a criticality for the community.

Table 1: Critical Infrastructure Sectors (FOCP 2014b)

Public Administration • Foreign representations and headquarters of international organizations • Cultural property • Parliament and other government facilities • Research institutes	**Transport** • Air transport • Rail transport • Road transport • Water transport • Postal services
Energy • Natural gas supply • Oil supply • Power supply	**Public Safety** • Armed forces • Emergency organizations • Civil defence
Waste Disposal • Waste • Wastewater	**Water and Food** • Food supply • Drinking water supply
Financial Services • Banks • Insurance companies	**Industry** • Chemical and Pharmaceutical Industries • Machinery-, Electrical and Metal Industries
Public Health • Laboratories • Hospitals and medical care	**Information- and Communication Technologies (ICT)** • Information technologies • Telecommunication • Media

The wide range of CI sectors shows that not only power supply stations or armed forces are critical and further it does even not cover all the suppliers that might be also relevant for CI to operate properly.

What makes CI different or why should they be better protected? CI's are different because the impact of an accident, blackout or malfunction would have taken into effect on a large part of the population in Switzerland. Therefore it must be in the communities/public interest that these CI's are protected and secured against faults and sabotage (FOCP 2012b).

It's obviously that these reasons make them different to non-critical infrastructure businesses where a fault or sabotage has less impact on the community and their livelihood. Probability of occurrence of this kind of incident for CI's is in many cases low or even improbable but the impact on the ecosystem would be extensive. Especially cyber-attacks with less effort can have a significant impact on our social wellbeing (ENISIA n.d.).

3.2.1 Cases of Disruption

The following lines describe cases of disruption and what kind of cyber risks can be.

> **RO1:** Description of today's cyber risks for CI's

The vulnerability of CI's is very various as the attack can be intended (attack by a terrorist, theft) or unintended (human error, malfunction etc.) and also depends on the target. Not every risk in an enterprise must be prevented or mitigated in the same way but critical risks for the interdependent network of CI's have to be addressed adequately (Wenger 2014).

One important question is: "Are CI's a target for sabotage, information espionage or other crime?" Ernst&Young Information Security Leader Ken Allan (2013, p.23) said generally: "Cybercrime is the greatest threat for organizations survival today."

Gartner (Pettey & Goasduff 2010) predicted in 2010 that by 2015, G20 nation's CI would be disrupted and damaged by online sabotage. Online attacks are highly efficient as they can target multiple systems for a maximum impact (Pettey & Goasduff 2010). Distributed denial-of-service (DDoS) attacks are primitive but effective ways to disturb online communications (Leimbach et al. 2014, p.65) and even if they address just on of many customers of a provider like Swisscom, it can have a large impact on the whole network service of Swisscom, mentioned Lütz in the interview (2014).

Current Gartner report "Gartner Reveals Top Predictions for IT Organizations and Users for 2014 and Beyond" mentioned that by 2020 75% of sensitive data protection will fail and the public will have access to it (Rivera 2013). Vulnerabilities are in all infrastructures and may expose sensitive information that can be exploited by attackers. Attackers that have been targeting CI for a long period are increasingly using the cyber space (Hämmerli 2010, p.23). This shows the trend in information security and may lead to another WikiLeaks (Assange 2006) of sensitive business data?

According to statistics provided by the Organisation for Economic Co-operation and Development (OECD), Switzerland is one of the leading countries by patent applications worldwide which is an indicator for innovation power (OECD 2011). Gain access to corporate intellectual property like innovation technology plans can be one of the attackers target. It is one of the main fear of industrial companies in Switzerland to find their

innovative products copied one-to-one on the market produced in other countries (Lütz 2014).

Leads to the question of data protection and whether to store the data in the cloud or locally as according to Eduard Snowden (2013) the USA National Security Agency (NSA) can frequently find ways to decrypt encryption or even more efficient get access to data stored on platforms of US-based providers through the patriot act (FinCEN 2001). Attacks by hackers, human failure or physical catastrophes (fire, earthquakes) represents scenarios where a permanent data loss can be the result if the data is stored in the cloud and therefore have to be taken in to account (Leimbach et al. 2014, p.65).

But also local storage of information in the enterprise network has its security vulnerability because according to the interview with an Operational Security Manager of a Swiss financial institute (Anonymous 2014), the hardware can also be infiltrated with malware that exploits over a certain time after installation. One of the most famous and mentioned "Zero-Day" attack of the last years was Stuxnet (Falliere et al. 2011), which attacked the industrial programmable logic controllers of centrifuges for separating nuclear material in the Islamic Republic of Iran.

Lehmann & Kempe (2014, p.1) point to the fact, that cyber-risk management needs to focus not isolated to the internal IT but also to external environments of the supply chain, outsourcing partners, upstream infrastructure and external shocks to be able to aggregate the risks. Malfunction of the Internet can have cascade effects to interconnected infrastructures of banks, water systems, cars, medical devices, transformers or power stations (Lehmann & Kempe 2014, p.3). Smaller CI's are equally affected of protection activities then larger CI's as they are also part of the big picture (Habegger & Kmiecik 2010, p.6). But they may have lack of resources (financial/staff/knowledge) to fulfil the needed performance in this area (Wenger 2014).

Several big accidents or attacks involving CI's happened in the past. The following Table 2 shows some cases of disruption as examples with different route cause and damage potential.

Table 2: Cases of Disruption

Problem / Cause	Description
Software Problem	Due to a software problem during a software launch in March 2003, the whole flight control system of Japan was broken and several 100 flights were cancelled. It took days to bring the system up and running again. (FOCP 2007, p.6)
Sabotage	A 49-year old attacker was able to infiltrate the computer controlled water supply system of Queensland (Australia) in March and April 2000. He was then in the position to flood millions of litre of wastewater into rivers, parks and even the water system of hotels. (FOCP 2007, p.6) Traffic light controls on four busy L.A. corners in August 2006 were the target of sabotage and caused major traffic jams for four days. (Rid 2013)
Blackout	In September 2003 a complete power outage of the energy system in Italy happened after a transit power line in Switzerland was broken due to a broken mast. This caused a financial damage of approximately CHF 185 Mio. It was one of four large-scale power outages in only seven weeks at this time. This reveals lacks in the mashed electricity network and shows the potential for terrorism action in this field as well which dependencies on electricity exist. (FOCP 2007, p.5)

The report "Erster Bericht an den Bundesrat zum Schutz Kritischer Infrastrukturen" of FOCP (2007, p.7) especially outlined Governmental, Economic, Traffic, Energy and Information Infrastructures as attractive targets for terrorism acts and asymmetric warfare as these environments, due to economic reasons, can't be protected in the same way as i.e. military infrastructures. Also electronic voting systems in Switzerland are one of several future potential risks mentioned by FOCP (2014a).

3.2.2 Strategies and Organizations for Critical Infrastructure Protection and Cyber Security

CIP and cyber security are on the roadmap of several countries including the USA, Germany, Netherland or Switzerland (FOCP 2007, p.17). The following section outlines ongoing and already finished strategy programmes in Switzerland.

> **RO3:** Evaluation of current Swiss programs and strategies

3.2.2.1 Critical Infrastructure Protection Strategy

CIP is nothing new but for a better cross-sectorial coordination and consolidation of the efforts in this area, FOCP assigned a task to the CIP Working Group to compile a basic CIP Strategy. The Federal Council then finally approved the CIP Strategy in 2009. Its main goal is to define common strategic goals, relevant principles and what measures have to be taken in the area of CIP. (FOCP 2009b)

In a first step the document describes the goal and purpose of CIP as: "The goal of critical infrastructure protection is to reduce the likelihood of occurrence and/or the extent of damage incurred in a disruption, failure, or destruction of critical infrastructures at the national level, and to minimize the duration of downtime. These measures constitute an effective contribution to the protection of the population and its livelihood." (FOCP 2009a, p.3)

The principles focus on Integral Risk Management, All-hazards approach, Resilience, Maintaining proportionality and subsidiarity. It outlines the responsibility of the private sector where 80% of the CI's are located. Public authorities are, according to the strategy document, mainly responsible to protect their own CI's and additionally support the operators of CI's in the private sector. Further it states that the CIP strategy follows an all-hazard approach including all relevant risks and do not focus on a particular one. These risks then have to be assessed with a common threat and risk assessment and measure them in the areas of prevention, preparation, intervention, recondition and reconstruction. (FOCP 2009a, p.4)

Coordinating activities between authorities, the cantons and operators of CI's are in the responsibility of the FOCP. Communication and information within these stakeholders, briefing the Swiss Federal Council or chairing the working group on CIP is of vital importance. (FOCP 2009a, p.6)

It is prominently stated that a superordinate legal framework for comprehensive implementation of measures is lacking and individual sectorial legal regulations covering only partial aspects of CIP issues. When ever possible existing foundations should be used and if they are insufficient, the following instruments are available (FOCP 2009a, p.7):

- **Directives**: (legally) binding prescriptions on fulfilment and verification of an agreed protection goal.
- **Incentives**: Promotion of measures designed to encourage the voluntary fulfilment of a protection goal by operators of CI's.
- **Public-Private Partnership** (PPP): Promotion of cooperation between public authorities and private operators of CI's. PPP projects take into account the needs of the operators as well as those of the state in order to realize joint solutions.

Overall it can be said the CIP strategy does not include mandatory directives or measures CI's have to be compliant with. Sectorial regulations and policies should implement the CIP strategy but the responsibility of coordination and communication is the main task of the FOCP. Without adequate collaboration between public and private sector representatives, no effective CIP policy can be put in place (Hämmerli 2010, p.20).

3.2.2.2 Cyber Security Strategy

In addition to the CIP Strategy (see section 3.2.2.1) a national strategy for the protection of Switzerland against cyber risk has been published in 2012 by the FOCP to address the fundamental changes that have been brought by the use of information and communication infrastructure in the private sector, state and society. The Cyber Security Strategy outlines that it is to be expected that the risk of disturbances, manipulation and specific attacks by criminal, intelligence, politico-military or terrorist motivated people/institutions will increase in the future. (FOCP 2012a)

The following strategic goals have been defined:

- Early identification of threats and dangers in the cyber field
- Improvement of the resilience of CI's
- Effective reduction of cyber risks, especially cyber crime and cyber sabotage

Reducing cyber risks is based on acting with personal responsibility, cooperation between public and private sector and cooperation with foreign countries as well including players from administrative, technical and top management levels. (FOCP 2012a, p.3)

The strategy defined therefore seven spheres with concrete measures including (1) research and development, (2) risk and vulnerability analysis, (3) analysis of the threat landscape, (4) competence building, (5) international relations and initiatives, (6) continuity and crisis management and (7) legal foundations. It is mentioned that these measures should be implemented by federal agencies and their partners and verified by a coordination unit established in a federal agency. (FOCP 2012a, p.4)

The coordination unit will only exist until complete implementation of the strategy on not clearly declared scope of involved enterprises and organizations within the next four to six years. Reporting and Analysis Centre for Information Assurance (MELANI) will take over the coordination and upon completion of implementation if necessary. (FOCP 2012a, p.41)

3.2.2.3 MELANI

MELANI is a Swiss Government Organization founded in 2004. It is a platform for partners of CI environments who work together to increase the security of computer system and the Internet to improve the protection of CI's. It has the main ambition to coordinate activities within the member enterprises of MELANI and its partners and to communicate information to interest groups if needed. (MELANI 2004)

MELANI (2012) inform their core member about current critical security issues and provide best practice recommendations, which than made partially available with a delay to the public (Schneider 2014).

MELANI is well known in the industry. All participants of the survey in the appendix (see section 10.1) have stated that they know the organization but i.e. Swisscom has neither an internal nor external requirement or driver to be part of it as Lütz said in the interview (2014).

Stakeholders of CI's mention negative points of MELANI in the survey that it is "best effort", the large number of participants makes it difficult to discuss interactively (Anonymous 2014) or that only members of the core MELANI group get exclusive or precociously information about security incidents (Schneider 2014).

Positively experiences noted by the survey participants was the MELANI supports actively in case of incidents (Anonymous 2014).

In general the participants of the survey mentioned, that the exchange of security attacks and threats is a matter of trust (Anonymous 2014) and delicate to share vulnerabilities to others with the fear that this information fall into wrong hands (Schneider 2014). MELANI is one organization among others as the financial institutes have their sector specific expert group BankenCert (Anonymous 2014) or SRG SSR is member of the Technical Committee of the European Broadcasting Union (Schneider 2014) where they exchange information in a trusted environment. The national cyber security strategy (FOCP 2012a, p.3) addresses this problem and stated that mutual exchange of information on permanent basis is to create trust and transparency.

3.2.3 Summary

A large and heterogeneous group of enterprises are part of CI in different sectors (FOCP 2009b) that includes among others power supply, water systems or information and communication systems.

The FOCP has defined that Switzerland is highly dependent on CI's that ensures the supply of crucial goods and services. Impacts on one CI can have a domino effect on other CI's and it is therefore important to look at the CI's as a whole to take interdependencies into account. (FOCP 2009b)

Different types of attacks and accidents happened in the past and had resulted in significant impact on the population and financial damage (see Table 2).

On governmental level there is an increased attendance for the need of CIP and a Cyber Security Strategy. The described programmes improve the cross-sectional coordination and explore the interdependencies of CI. (FOCP 2009b)

A conclusion of the survey is that these programmes do neither sufficiently define actions nor mandatory technologies; therefore they have a high level view. It's still based on a best effort approach (Anonymous 2014). The Cyber Security Strategy of the FOCP (see section 3.2.2.2) defines compliance verification but does not provide a list of target enterprises that should fulfil the measures in the next years. Define penalties or enact a new law addressing this topic is equally not part of the strategy.

According to Leimbach et al. (2014, p.66) it is not possible to achieve a high level of confidentiality and a minimum security standard without a secure computing base – therefore the standards may have to be defined and applied on a mandatory base by the government or international commissions for at least CI's. Additionally Gartner said that updates of regulatory standards are faster released than enterprises can implement them what resulted in confusion and decision uncertainty for affected industries. The recommendation for this situation is to separate the technology standards and guidance from regulatory guidance. (Perkins 2013)

3.3 Information Security Instruments

An extract of best practice instruments as well guidelines for information security and CIP in Switzerland is described in this section. This selection of instruments was mentioned in interviews with stakeholders of CIE's (see section 10.1) and gives an overview of the diversity of different CIE.

RO2: Observation of used instruments in CIE's to prevent and mitigate CI risks

Different definitions of information security exist but in this research the definition described by the Information Systems Audit and Control Association (ISACA) combined with the definition of the US National Institute of Standards and Technology (NIST) are used.

Definition: "*Ensures that within the enterprise, information is protected against disclosure to unauthorised users (confidentiality), improper modification (integrity) and non-access when required (availability).*" (ISACA 2012a)

Another but congruent definition provided by NIST:

Definition: *"Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity (...), confidentiality (...) and availability (...)."* (NIST 2006)

Both organizations described confidentiality, integrity and availability (CIA) with the same words:

- **Confidentiality** means preserving authorized restrictions on access and disclosure, including means for protecting privacy and proprietary information
- **Integrity** means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity
- **Availability** means ensuring timely and reliable access to and use of information

NIST and ISACA are well-established organizations; both release well-known and respected material in the area of information security and therefore the same terminology and definitions are used in this research.

The list of instruments is composed based on experiences from interviews with stakeholders of CIE's (see section 10.1) as well on secondary literature. The list is ordered by relevance for Swiss CIE's starting with (1) the local Swiss CIP Guideline released by the Swiss

Governance followed by the well-known frameworks in Western Europe (2) COBIT5 for Information Security and (3) International Organization for Standardization ISO2700x which were mentioned several times in the interviews with involved stakeholders of CIE's. Additionally considered in this scope are the US frameworks (4) NIST Cyber Security and (5) North American Electric Reliability Corporation (NERC) CIP Compliance as the US organizations are working on these topics for several years, they can act as benchmarks and might be relevant as well helpful for Switzerland.

3.3.1 CIP Guideline

CIP Guideline (SKI Leitfaden) was initiated by the Swiss Federal Council explicitly to protect CI's by strengthen their ability of resilience and minimize the time of outage or avoid it entirely. The draft version was released in February 2014 by the FOCP. Its context is a broader view on all CI sectors with their dependencies to cover not enterprise (operational) but national risks (complex dependencies between CI's). There is at the time being no available guideline with an overall perspective for CI's. (FOCP 2014c)

This work is based on well-known holistic risk, crises and continuity management approaches but does not formulate regulations or obligations for CI providers. CIE´s can use this guideline to measure current security level and identify vulnerabilities. Its focus is not only on information security or cyber risks. CIP Guideline is part of the holistic CIP security management of FOCP.

Reference to the survey in the appendix 10.1: Nick Wenger (2014) mentioned the CIP guideline in the interview and noted that this paper is not as well-known as the Cyber Strategy described in section 3.2.2.2. Mühlheim (2014) mentioned that Swissgrid is involved in a pilot project to prove and improve the CIP guideline. Others didn't mention that they use or know this guideline.

3.3.2 COBIT5 for Information Security

COBIT5 for Information Security is a specialization of the COBIT5 Framework. COBIT 5 (ISACA 2012a) provides a comprehensive framework that assists enterprises in achieving their objectives for the governance and management of enterprise IT to create optimal value from IT by balancing benefits and optimizing risk levels and resource use. (ISACA 2012b, p.13)

The Information Security specialization links information security with generic enterprise goals including:

- Ensures continuously availability of services and systems to internal and external stakeholders
- Be compliant with the increasing number of laws and regulations as well with internal polices on information and system security
- Align major frameworks
- Reduce complexity and increase cost-effectiveness due to improved integration of information security standards (such as ISO27001 or PCI DSS) and sector-specific guidelines

This framework is relevant for the research project because it also focus on the importance of nation CI's, which are depended on information systems. It is also mentioned, that successful intrusions can result in a significant impact to economies or human safety and that industrial espionage can trade secrets to be imitated (ISACA 2012a).

The framework does not dictate any implementation details for specific situations as, due the nature of the enterprises, they have different risk appetite based on the environment where the operate and their risk stance (ISACA 2012a). It does focus on what is to do but not on how and therefore an enterprise needs to hire experts to interpret, adapt and implement the framework (Mingay et al. 2012).

Gartner said, that the current version of COBIT5 (including Information Security specialization) is much broader and therefore more complex than its previous version. However the broader scope could overwhelm new users and inhibit its adoption. Further it is mentioned that it makes acknowledgments but does not provide useful guidance on sustainability. (Mingay et al. 2012)

Reference to the survey in the appendix 10.1: Nobody of the interviewed stakeholders of the survey mentioned that they use COBIT5 or COBIT5 for Information Security in their environment. Their focus might be exclusively on ISO2700x described in the next chapter.

3.3.3 ISO2700x

ISO2700x standards are well known in investigated CIE's and were originally released by the UK Government and later adapted and reserved by the International Organization for Standardization (ISO). Its focus is on Information Security Management Systems (ISMS).

ISO27001 provides requirements for establishing, implementing, maintaining and continuously improving an ISMS (ISO 2013a) whereas ISO27002 is a code of practice for information security including several potential controls and control mechanisms that supports the guidelines of ISO27001. It includes general principles for initiating, implementing, maintaining, and improving information security management within an organization. (ISO 2013b)

These standards are a good starting point for investigation in this research as they are well known and accepted in the industry. It covers a broad range of information security not specific on information technology (Schneider 2014).

Reference to the survey in the appendix 10.1: All interviewed CIE stakeholders mentioned that they align their ISMS to ISO2700x but there is no regulation that requires an ISO certification in this area. I.e. SRG SSR approach is to be compatible with ISO2700x standards and use the beneficial parts of them but they are fare away from a certification yet as it is a lot of paper work mentioned Schneider (2014).

Other ISO2700x standards that were not mentioned during the interviews but are defined: (1) ISO27003 is not released yet but will offer a guidance for implementing ISMS, (2) ISO27004 describes the metrics for controls mentioned in ISO27002, (3) ISO27005 is a methodology for information security risk management and finally (4) ISO27006 is a guidance for accreditation of organization offering ISMS certification.

3.3.4 NIST Cyber Security Framework

NIST Cyber Security Framework (CSF) was released in February 2014 by the U.S. Department of Commerce as a reaction to the call of the U.S President Executive Order 13636. Its focus is on using business drivers to guide cyber security activities with to goal that cyber risks get part of the organization's risk management process. Regardless of size the CSF should be applicable to any CI organizations to improve their security level and resilience. (NIST 2014, p.3)

It is distinguished that the framework approach does not met all requirements to manage cyber risk for CI's as they will continue to have unique risks based on different threats, vulnerabilities or risk tolerances (NIST 2014, p.4).

CSF is a voluntary framework (NIST 2014, p.3) and not a regulatory guidance nor a checklist for regulatory compliance. Gartner (Perkins 2014, p.2) stated that this can leave the governance with little power to mandate changes in cyber risk management.

Gartner's (Perkins 2014, p.2) recommendation is to apply standards that are well-accepted by specific industries and avoid compliance-based decisions from the CSF guidance in its current state as it is missing key components. Further it does not replace operational frameworks like COBIT5 or ISO2700x and is not related to NERC CIP standards. It can support an enterprise to align and integrate a cyber risk management across corporate and industrial control requirements.

Reference to the survey in the appendix 10.1: CSF is the most recent publication in this area released in February 2014 and therefore it is not implemented or used by any company attending the interviews in the appendix. Ongoing projects of the Swiss Governance will take notice of it and adopt reasonable sections if appropriate (Wenger 2014).

3.3.5 NERC CIP Standards

North American Electric Reliability Corporation (NERC) is a non-profit corporation with the major responsibility to ensure power system operators remain qualified and proficient by work together with all stakeholders developing standards for power station operation. The CIP Reliability Standards requires operators of Bulk-Power Systems to comply with specific requirements to protect critical cyber assets. It defines among others how to (1) report

sabotage acts, (2) identify cyber assets or (3) create recovery plans for critical cyber assets. (NERC 2013)

Different to other instruments mentioned in this section NERC CIP standards affected companies have to be compliant with them driven by the government (with version 4 by April 2014) and shows that there is real pressure from the government to achieve these standards.

NERC published in 2009 that the electrical grid is not adequately protected against cyber-warfare (2009).

Reference to the survey in the appendix 10.1: Even if NERC CIP compliance is only required for the US industry, it is used by Swissgrid to achieve a minimum setup in terms of cyber security. It is a good starting point to cover the basics CIE's has to fulfil (Mühlheim 2014).

3.3.6 Comparison

Table 3 shows for each instrument the area and characteristics that make them relevant for further research.

Table 3: Overview Information Security Instruments

Instrument	Region Scope	Characteristics
CIP Guideline	Switzerland	Holistic CIP focus; well-known in Switzerland; no mandatory compliance checks; measure maturity level
COBIT5 for Information Security	Global / Europe	Information Technology Information Security focus; well-known; no mandatory compliance checks;
ISO2700x	Global	Overall Information Security focus; well-known; no mandatory compliance checks;
NIST Cyber Security Framework	USA	Specific Cyber Security focus; new; benchmarking
NERC CIP Standards	North America	Cyber Asset focus for Power Systems; Mandatory compliance checks; established in USA;

4. CASE STUDY

Case study research is used to investigate CIE's with the objective to disclose potential problems in information security with regards to cyber risks and usage of existing instruments mentioned in section 3.3.

This part of the research is leaned on Yin's "Case Study Research" (2009) as this approach is dealing with case studies and describes especially the handling with multiple case studies. Yin is recognised and referenced in many scientific articles, reports and journals with several versions of his case study research. (Zucker 2009; Asprion 2013; Kohlbacher 2006)

The interviews based on case study approach have been carried out from April till July 2014. Various group of CIE's from different sectors including financial services, energy, information and communication technology (ICT) and public administration build the unit of analysis (Yin 2009, p.31). The answers from the questionnaire are used to carve out potential problems with information security with regards to cyber risks in practice to get the basis for research objective 4 "Exploration of discrepancies of existing Swiss programs and strategies, used instruments and the information security need of CIE's" (see section 1.3).

Transcripts of the interviews are attached in the appendix (see section 10.1).

4.1 Case Selection

In conformity with Yin (2009, p.54) each case in a qualitative multiple use case must be carefully selected to get a significant result. Yin (2009, p.54) mentioned two ways of use case selection for qualitative research:

a. Predicts similar results (a literal replication) or
b. Predicts contrasting results but for anticipatable reasons (a theoretical replication).

Letter b) of Yin's proposals above is used for this research as contrasting results can be expected due to the variety of different CI's (see section 10.1). Used instruments and standards in different enterprises of diverse sectors may vary strongly due to a different background of existing regulatory, different environment and other aspects.

Only a small group of CIE's are selected because of difficulty to find willing CI experts in the area of information security who wants to provide internal information about this sensitive topic. Nevertheless the selection includes enterprises across different sectors to cover a wide range of CI's.

The following criteria are applied:

1) Critical Infrastructure:
   Only CIE's according to the list of CI sectors of the Swiss Government (FOCP 2014b) are considered for this case study.
2) Swiss based nation-wide enterprise:
   CIE's with a nation-wide influence have a significant impact in the research area and therefore the focus is on Switzerland-based enterprises that offer services to the Swiss community. International enterprises belonging to CI's for Switzerland i.e. technology company's providing "de facto" standard computer operating systems are not covered directly by this research.
3) External stakeholder:
   Beside the CIE's of target group 1 and 2, it is also helpful to get unembellished information based on experiences of partner, consultants or government officers who are directly involved and cooperated with CIE's that fulfil criterion 1 and 2. This group can also be considered as verification for statements of CI experts.

The interviewee scope is focusing on experts involved directly in information management, risk management or are board members in charge with risk management or information security tasks. Information security is a sensitive topic hence only five CI experts did agree to attend the case study (see section 10.1).

Derived from criteria definition above, four CIE's and one external stakeholder are selected (Table 4):

Table 4: Overview of CIE selection for case study research

Enterprise	Sector	Name / Position	Comment
Federal Office of Civil Protection[2]	Governmental Institute	Nick Wenger Project Manager Critical Infrastructure Protection	FOCP coordinates the implementation of the Swiss national strategy on CIP FOCP provides guidelines and information to CI
Financial Institute	Financial Institute	Anonymous Operation Security	Financial industry is already highly regulated and they have therefore experience implementing requirements by the regulation authority
SRG SSR	Media	Andreas Schneider Lead IT Security	Media and Broadcasting is important in an emergency case to provide relevant information to the population This sector is currently low regulated in terms of information security and therefore interesting for this research
Swissgrid	Energy	Andy Mühlheim CIO	Energy sector and especially the power grid provider Swissgrid are highly critical for Switzerland
Swisscom	Telecommunication	Mark Lütz CISO Outsourcing	Telecommunication is highly critical for Switzerland especially Swisscom as the biggest player in this sector in Switzerland

Selected use cases have common attributes:

- Population as consumer/customer
- ICT is crucial for operating their business (10.1)
- Large impact for the population in case of disruption (FOCP 2014c)

But the use cases differ in some aspects:

- Regulation authorities (FOCP 2014c, p.61)
- Criticality of corresponding CI sub sector (Figure 11)
- Size of CIE (number of employees; turnover)

[2] Different question were asked to the expert of FOCP as this department acts as an external observer and is also involved or responsible for several ongoing governmental projects mentioned in section 3.3.1.

4.2 Interview Guideline

The main objective of the case studies is to find existing information security, especially cyber security issues in CIE's and how they protect their assets. In addition it is important to know the usage of existing instruments in the area of information security to find common patterns between other CIE's.

The questionnaire is divided into six questions to get facts about the current situation in CIE's in the field of information security. A start question #1 sensitizes the interviewee with the topic to get appropriate answers to four main questions. In the end a termination question #6 has the aim to get a final statement about potential problems and closes the interview:

1. *In your opinion, is your enterprise part of CI's in Switzerland?*
   As a first question, the CI expert is asked to answer the question if in his opinion the enterprise is part of CI's and what are the critical parts for the Swiss population (FOCP 2014b). This question should sensitizing the interview partner with the topic of CI's.
2. *Which attacks on information assets did you face in the last 10 years?*
   Attacks on information assets show the attack vector and importance of protection. "Current international ICT infrastructure situation" report by MELANI is used as a reference guide (MELANI 2014). Further the expert should provide information about where the organizational or technical lacks are to investigate in the future.
3. *How do you prepare your information security environment against current risks?*
   Which effort did the CIE spent in the future to protect their information assets and how can they improve it. This is interesting to get common or contrasting behaviour in protection of their information assets and how much budget CIE spend for it (van Kessel & Allan 2013).
4. *Which regulations or internal guidelines with regards to information security exist in your area*?
   Different sectors of CI have different regulations if any (FOCP 2014c); question 4 should confirm this hypothesis.
5. *Which advantages and disadvantages would a common information security framework have to improve security*?
   As a follow up question to number 4, what do they make of a common framework (Aquilina 2014) or other common regulations for all CI adapted i.e. from NERC CIP Standards? (NERC 2013)
6. *What is the main challenge in information security in the next five years?*
   As finishing question, it is interesting to get their thoughts about future threats and challenges and where they see potential to invest (World Economic Forum 2014). If they do not see any problems with information security especially with cyber threats, the developed CIISM will not be relevant.

Aim of the interview is to get the minds of CI experts about their thoughts of today's information security and what are their concerns and challenges in this area. The questions are formulated in an open way within the topic borders to let the interview partner think about the topic in an open mind.

4.3 Outcome

Interviews were analysed by comparing and classify answers of mentioned concerned topics in more general terms. Questioned CI experts outlined several problems and thoughts about current and future situation regarding to mitigate or prevent cyber risks. Table 5 summarizes the outcome from the case study interviews and illustrates the most common mention topics of concerns and issues.

The following topics were frequently mentioned as answer on questions of section 10.1 and therefore selected for further investigations. Topic sequence is alphabetical and value-free.

- Awareness (Question 6)
- Cooperation / Education (Question 3)
- Funding / Costs (Question 5)
- Regulation (Questions 4, 5)
- Risk Management (Questions 3, 4)
- Technology (Questions 2, 6)

The used symbol ⊙ in Table 5 means, that this specific topic was mentioned in the answers of the corresponding CIE.

Table 5: Outcome Case Study Interviews

Topic	FOCP[3]	Financial Institute	SRG SSR	Swisscom	Swissgrid
Awareness	⊙	⊙	⊙	⊙	⊙
Cooperation / Education	⊙	⊙	⊙		⊙
Funding	⊙	⊙			⊙
Regulation	⊙	⊙	⊙	⊙	⊙
Risk Management	⊙	⊙	⊙	⊙	⊙
Technology			⊙	⊙	⊙

Following sub chapters describe the mentioned topics of Table 5 in more detail and refer to the relevant interviews and statements in the appendix (10.1).

[3] Different set of question were asked to the expert of FOCP as this governmental department acts for this case study as an external observer

4.3.1 Awareness

Awareness means: *"Activities which seek to focus an individual's attention on an (information security) issue or set of issues."* (NIST 2006)

All participants of the case study confirmed, their operational infrastructure is based on IT systems and therefore highly dependent on it. Awareness therefore means to be aware of what can happen and what are the current risks related to IT systems.

To adequately address these risks, the management has to be aware of it but management attention is a problem. Dependencies between IT and business must be formulated to get management attention. Costs are often a problem due to lack of management attention. Therefore it is hard to invest in security infrastructure or process proactively before an incident occur mentioned Lütz and Schneider (2014; 2014). Also Wenger (2014) noted that real outages and problems open a better "window of opportunity" to get management attention and address the risks sustainable. This statement is confirmed by past incidents of hacker attacks against the SRG SSR networks that has changed the management minds slightly and set cyber attacks on their agenda (Schneider 2014). The financial institute case study has shown, that the application of a security roadmap can improve the awareness of the management board and appropriate money can be spoken. (Anonymous 2014)

Another application of awareness is the customer (CI customers in this case are dependent CIE's and the population) understanding and recognition of quality in terms of sustainability and stability of CI's. Investments, among others, in information security components have to be done to operate these services (Mühlheim 2014).

4.3.2 Cooperation / Education

Cooperation means: *"Cooperation is the process of groups of organisms working or acting together for their common/mutual benefit (...)"* (Ray 2014)

Time is rarely available in fast changing environments of information technology to react on new upcoming threats. Therefore cooperation between CIE's can be beneficial for CIE's to share information and knowledge to prevent or mitigate risks adequately.

According to the interviews, governmental information platforms like MELANI (see section 0) are only partially used by CIE's. One reason could be that cooperation with MELANI is basically appropriate to get general information (Mühlheim 2014), active support and information in an emergency case (Anonymous 2014).

To increase the gain of MELANI, the Swiss Federal Office of Communication (FOCOM) as the regulatory authority of SRG SSR wants to consolidate risks and incidents to report them to MELANI. But sensitive incident data are currently not shared generally with others partners although it would be beneficial for all according to Schneider (2014). Sharing of incident information of your own environment is a sensitive topic and most of security experts are not willing to share confident data to an external organization. It was also mentioned in the financial institute use case (Anonymous 2014), that smaller groups of interest would be more appropriate to discuss confident topics.

Other sector-based cooperation exists in the broadcasting section as SRG SSR is not member of MELANI but other organizations like technical committee of the European Broadcast Union (EBU) (Schneider 2014). Also a smaller partner network is used in the financial services and power supply sectors to share and discuss common topics of interest (Anonymous 2014). Swissgrid works additionally together with governmental projects mentioned in section 3.2.2 (Mühlheim 2014). Additionally Lütz (2014) mentioned, that the dependency between providers is one of the main risks and therefore cooperation between involved CIE must have a high priority.

Education is "the act or process of imparting or acquiring general knowledge and developing the powers of reasoning and judgment (…)" (Dictionary.com 2014a).

Education of experts in the field of information security is important to define, integrate and develop security concepts in a CI environment. CIE's have to man their digital borders with people who have the same skill and determination as the attackers as technology is static but threats aren't (Assante 2014). But currently it is difficult to train IT security experts because of lack of instruction courses. (Mühlheim 2014) International cooperation in education and training can be a change to improve the availability of security experts. As a first step, Switzerland worked together with other countries (Netherland, Germany, Austria) while developing the guideline for CIP (see section 3.3.1) (Wenger 2014).

4.3.3 Funding

Funding means: *"Money provided, especially by an organization or government, for a particular purpose."* (Google 2014a)

Especially in this context: Who will fund the activities for implementing security? Who will pay for investments in security and related activities when the government define new laws and regulations? (Wenger 2014) Funding is nearly related with awareness as we as customers only will pay for something if we are aware of what we get. Costs must be shift to the consumer/customer if CIE's have to fulfil overall mandatory regulations (Lütz 2014).

This leads to the question: Who is the owner of the risk and who pays for it? I.e. the community is dependent on the network services of Swissgrid but the price tag does not reflect the real effort for risk mitigation. The community is not willing to pay additionally costs for security (Mühlheim 2014).

Additional costs will also arise for new education possibilities (Mühlheim 2014) and implementation of cooperation networks / organizations (see section 4.3.2).

4.3.4 Regulation

Regulation means: *"A law, rule, or other order prescribed by authority, especially to regulate conduct."* (Dictionary.com 2014b)

As described in the introduction (see section 1), CI's are important for Switzerland and a malfunction or damage of a CI's will have large impact on our community. Therefore the question of an overall mandatory regulation was asked to the participants of the case study. Would it help to get the awareness of the management and address current risks adequately? Compliance regulations can improve the pressure on management as external and internal auditors review the infrastructure, processes and organisation (Anonymous 2014). No controlling is applied due to lack of regulatory pressure at SRG SSR mentioned Schneider (2014).

The interviews have shown, that only the financial industry of all investigated sectors has a mature regulation. FINMA sets relatively strict and strong regulations for financial institutes (Anonymous 2014). Beside that, BASEL I/II has direct influence on the operational risk of financial institutes. Lower operational risk means lower liquidity is needed and can provide an incentive to improve operational risk topics. (Anonymous 2014)

Telecommunication providers do not have regulations in information security but Swisscom does apply partially FINMA regulations to be compliant as a provider for financial institutes. A common framework can be difficult to apply on all services of a company like Swisscom that has different parts (i.e. shared services) that are relevant for different customer specific regulations (Lütz 2014). A common framework is almost not possible as the environments are to diverse, i.e. FOCP has its internal strict regulations, as it is part of the military system mentioned Wenger (2014).

Currently there are no mandatory guidelines or requirements for all CI's in Switzerland as it is the case i.e. in the United States (see section 3.3.5 NERC). Each provider sets it own guidelines (beside some regulated sectors like financial services). General content is a disadvantage of mandatory compliance guidelines, which have finally be adapted to each single CI. (Mühlheim 2014)

Overall, it would be helpful to have minimum requirements for CI's in terms of information security and especially in this case for cyber security. But costs of implementing minimum requirements should not be underestimated and how this is funded (see section 4.3.3) (Anonymous 2014). Also Schneider (2014) stated that it would make sense to even extend a minimum standard set of requirements in the area of cyber security to all operator of Internet connected services.

4.3.5 Risk Management

Risk Management means: *"The technique or profession of assessing, minimizing, and preventing accidental loss to a business, as through the use of insurance, safety measures, etc."* (Dictionary.com 2014c)

Risk management is part of almost every guideline or framework in information security. Therefore the correct usage and implementation is important. Current cyber risks must be recognized and addressed with adequate risk management activities (see section 3.1).

Awareness (see section 4.3.1) is essential for a successful risk management to have management attention and budget for addressing and tracking cyber risks.

For example the use case financial institute has shown an established risk management including IT as a risk. I.e. malware attack is recognized as large risk. Operational risk management is also more and more important. As these IT risks are defined as risks, they are also addressed in Business Continuity Management (BCM) and Service Continuity Management (SCM) (Anonymous 2014). Media companies do not have similar regulations or compliance requirements as financial institutes do. This makes it difficult to get awareness or define and mitigate risks. To define a risk at SRG SSR takes months – this is not acceptable for high volatile and dynamic cyber environment. (Schneider 2014)

CI risk management has to deal with the situation that the enterprise is basically vulnerable and has to be prepared to mitigate and react on these attacks especially against cyber risks (see section 3.1) (Mühlheim 2014). Mühlheim (2014) mentioned that risk management is often too weak because it doesn't cover the End-to-End view including i.e. energy supply. The risk of power outage has to be covered in every at least CI's risk management and CI's should invest in mitigation of common risks.

Cyber risk management on enterprise level require improved methods to deal in line with broader enterprise risk management practices. Digital connectivity becomes a new norm in economies and societies and therefore cyber risks need to be normalized and monetary quantified. Collaboration among other enterprises and sharing of ideas (World Economic Forum 2014, p.41)

4.3.6 Technology

Technology means: *"The application of scientific knowledge for practical purposes, especially in industry."* (Google 2014b)

The term technology is used for technical implementations, techniques or machines etc. "Some gear isn't even designed to be upgraded. There is a lot of ICS equipment still being produced today that has no firmware update mechanism." said K. Reid Wightman director of Digital Bond Labs (Mimoso 2014). Industrial systems do not have a rugged design and therefore may not protected against external attacks if connected to the Internet. Manufacturing companies should be discharged on their duties (Anonymous 2014).

May manufacturer should be internationally certified to produced secure systems and only certified products are allowed to be used in Switzerland's CI's.

Which part of the environment is important and critical? Are customer data or/and operation of the network important (Wenger 2014). Separation into an office network and a data centre network with all important control and operating networks might make sense (Mühlheim 2014). The digital wave consolidates classic operational environment with IT office networks and connectivity to the Internet (Schneider 2014).

Also in scope of technology challenges: New business cases i.e. like machine to machine (machine2machine) communication or cloud services can create new attack scenarios where a CIE risk management must react accordingly. (Lütz 2014)

4.4 Summary

Case study research distinguished the six main problem topics described in section 4.3. The interviews with the CI experts gave lot information where the CISSM prototype has to focus on.

Beside the main topics disclosed by means of the case studies, some general changes in information security will challenge CI's information security in the future and should be therefore considered while developing CIISM. Table 6 outlines mentioned challenges in the future by CI expert (see section 10.1)

Table 6: Challenges in the future

Topic	Description
Scope of criminal activities	In the past, criminal activities had the aim to get money from specific targets. Today's threat landscape is more global like i.e. widespread DDOS attacks based on common vulnerabilities of software/hardware are exploited. Whereat the attacks are more political or business oriented. Correlation of events and information is important to combat these risks but on the other side convey risks of espionage by national intelligence services. (Lütz 2014)
New technologies	New technologies like mobile strategies, BYOD or cloud services will raise new challenges in the area of information security in the future. (Lütz 2014)
Digitalisation of ICS	Current ongoing challenges are among others the digitalisation of ICS. ICS are more than ever connected to IT systems and the Internet and therefore more exposed and vulnerable against cyber threats. Also a common issue is the human being – the least element in information security attacked by social engineering or disregarding security policies etc. (Schneider 2014)

5. PROTOTYPE CIISM

CIISM addresses current issues in information security especially for cyber risks. It is recommended that CIE's and the government of Switzerland align their work to this model to improve the agility and ability to prevent or mitigate damage through information loss or manipulation (see section 1.3).

Inputs by CI experts disclosed weaknesses in diverse areas of information security (Table 5). These areas are selected as main components of the CIISM prototype. Modelled analogous to COBIT5 (ISACA 2012b, p.27) the components are called enablers (Figure 9).

Enablers have common characteristic of influence something whether it will work or not. Enablers are critical topics for CIP information security with regards to cyber risks – if one enabler is not considered, CIISM may not work. CIISM exists of six enablers that have dependencies among one another but no sequence or priorities are defined. Enablers need the input of other enablers to be fully effective and vice versa.

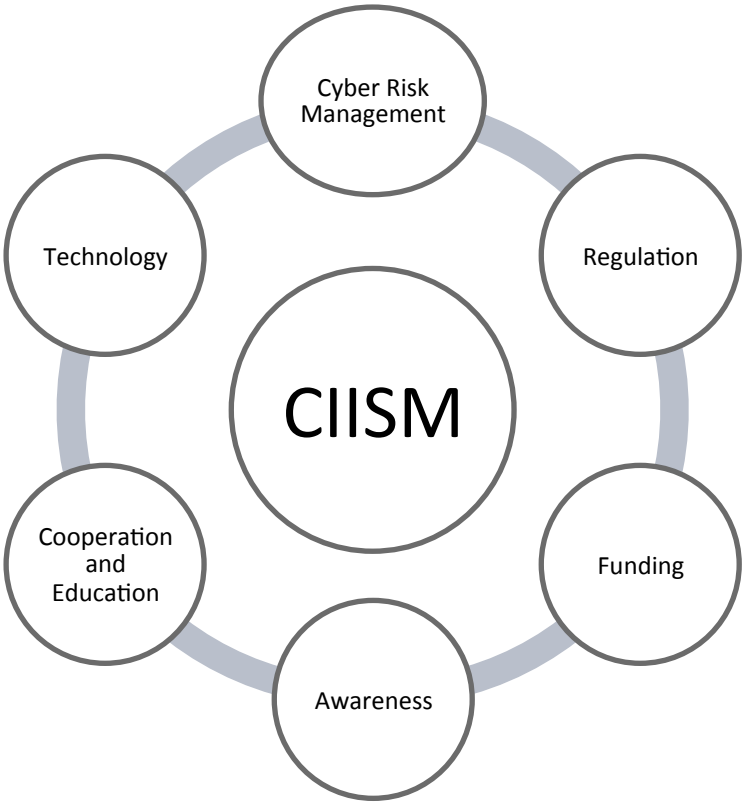

Figure 9: CIISM Enabler Overview

Following steps are used to build the framework:

1. Preliminaries: Preliminaries have been worked out to illustrate which enablers can be addressed in which way with existing instruments.
2. Enablers: Enablers define and describe the categories, which were identified to address today's issues in cyber security of CI's.
3. Application: Application describes the steps how to apply CIISM in practice of CIE's and related organizations.
4. Validation: Validation of the CIISM prototype has been done by questioning CI experts

5.1 Preliminaries

A prototype for prevention or mitigation of cyber risks for CI's has to address the issues described and categorized in section 4.3. In the following lines the required preliminary work is outlined to show how selected information security instruments (see section 3.3) can support disclosed issues.

> **RO4:** Exploration of discrepancies between existing Swiss programs and strategies and issues of CIE's

Each of the instruments is summarized in a table with focus on its content and if it addresses the mentioned problems of CIE's covered by the enablers. Additionally the instruments were investigated with keyword search if any section covers the specific problem. Some of these instruments are part of a holistic security management framework and may therefore address some superordinate topics that are not considered in this paper.

Following arrow symbols (Table 7) are used to visualize the usefulness to gain improvement to the current situation in information security for each specific issue topic:

Table 7: Symbol description

Symbol	Description
🡻	Not useful or no benefit
🡺	Marginal or partial benefit
🡹	Possible solution or approach for benefit

5.1.1 Awareness

Missing awareness of information security and management attention for this topic is mentioned in the interviews several time. How can awareness be improved? Which actions have to be taken to get management attention? Table 8 shows supporting parts of existing instruments.

Table 8: Awareness Instrument fulfilment

Instrument	Content	Authors assessment
CIP Guideline (FOCP 2014c)	Stated that risk management is important to get management attention Does not explicitly explain how to get management attention; it's in the responsibility of the management to verify the risk management Is designed that CIE's and the corresponding regulatory sector authorities have to submit their risk identification	Guide the CIE and regulatory sector authorities to implement risk management but not explicitly how to implement a cyber risk management – therefore only slightly improvements to current situations in investigated use cases ➔
COBIT5 for Information Security (ISACA 2012a)	Provides information about how to establish principles and polices Recognizing pain points: quick wins with the most added value have to be shown to the management to gain widespread senior executive commitment for other security relevant investments Defines what documents are relevant for management decision base to be prepared to get management attention Provides security awareness content for employee training: knowledge base, collaboration tools etc.	Describes how to get management attention with pain points and what documents should be delivered to the management – could be a first step to get management attention Provides security awareness content tools for employee attention ↑
ISO2700x (ISO 2013a)	ISO27001 (5.2.2) describes the importance of information security awareness trainings for employees	Includes awareness and skills training to get employees awareness but does not focus on management attention ➔
NIST Cyber Security Framework (NIST 2014)	Focus' on risk management based on business drivers what can help to get management attention Awareness training for employees is part of the core framework described in section PR.AT of the Cyber Security Framework	Describes how to link cyber risks with business drivers to get management attention Awareness training is one specific discipline of the framework ↑

NERC CIP Standards (NERC 2013)	Determines that personnel with access to security zone have to security awareness (CIP-004) Explicitly mentioned the need of general recurring security training for all employees with access to security zone (CIP-004) which raise the understanding for information security	Includes awareness and skills training to get employees awareness but does not focus on management attention ➔

5.1.2 Cooperation / Education

How can the cooperation between CIE's, the government and other stakeholders be improved? Table 9 shows supporting parts of existing instruments.

Table 9: Cooperation instrument fulfillment

Instrument	Content	Authors assessment
CIP Guideline (FOCP 2014c)	Outlines the cooperation of regulatory agencies and government to delegate tasks CI sector organizations like association of banks should work out solutions and time consuming tasks to support smaller CIE's and avoid heavy costs	Cooperation is mentioned in the guideline ➔
COBIT5 for Information Security (ISACA 2012a)	Information security monitoring is part of the "Services, Infrastructure and Application" Enabler	Does mention incident reporting on the edge but not detailed 🡻
ISO2700x (ISO 2013a)	ISO27001 (A.6.1 / A.6.2) explain actions for cooperation / communication to authorities and other relevant organizations	Includes actions of general communication between relevant organizations and authorities but not explicitly defined what content should be shared ➔
NIST Cyber Security Framework (NIST 2014)	Includes an explicit action: communicate among internal and external stakeholders about cyber security risk Provides a common language to communicate requirements among interdependent stakeholders responsible for the delivery of essential critical infrastructure services NIST Cyber Security Framework is not explicitly dependent on U.S. specific requirements and therefore usable in any other country	Does provide a common instrument to compare risk: risk profiles are useful to communicate your risk strategy May can be used as common framework in international CI task forces 🡹
NERC CIP Standards (NERC 2013)	Includes discipline about identify and report cyber security incidents (CIP-008)	To report incidents is a first step but does not claim to report incidents to national / international cyber security task force 🡻

Cooperation is also related to the area education of needed experts and training of employees but differs from cooperation for information sharing and therefore a separate table (Table 10) is used for education:

Table 10: Education instrument fulfillment

Instrument	Content	Authors assessment
CIP Guideline (FOCP 2014c)	Education of employees, training, risk communication etc. is an integral part of the CIP guideline	Includes education of employees but does not solve current issue of education lack (security experts) ➔
COBIT5 for Information Security (ISACA 2012a)	"People, skills and competencies" enabler is part of COBIT5 for information security. The goal is related to education and qualification levels, technical skills and experience levels	Usable role description including skill requirement etc. for relevant information security positions Does not solve current issue of education lack ➔
ISO2700x (ISO 2013a)	ISO27001 5.2.2 describes that the organization must ensure skills by trainings or other measures	Describes tracking methods and that an organizations have to ensure trainings but does not provide a solution for current issue: lack of training positions ➔
NIST Cyber Security Framework (NIST 2014)	Mentioned the importance of trained people	Does not solve current issue of education lack and no road map how to get trained people in the future ➔
NERC CIP Standards (NERC 2013)	Explicitly mentioned the need of general recurring training for all employees with access to security zone (CIP-004) No information about training for security experts	Useful: Requires minimum level of information security knowledge to employees with access to security zones ➔

5.1.3 Cyber Risk Management

Which instruments mentioned risk management with focus on cyber risks? Is there any description of cyber risks or action on how they should be addressed? Table 11 shows supporting parts of existing instruments.

Table 11: Risk Management instrument fulfillment

Instrument	Content	Authors assessment
CIP Guideline (FOCP 2014c)	Leaned on standard risk and crisis management methods Not specific on IT or cyber security risks and more high level risk management	Helpful to define high level risks and calculate impact and damage Does not address specific issues in risk management in this context ↓
COBIT5 for Information Security (ISACA 2012a)	Defines the role enterprise risk management committee (C4): Responsible for the decision making of the enterprise to assess, control, optimise, finance and monitor risk from all sources Defines the skill information risk management Information security review reports: • Threat analysis • Vulnerability assessment	Useful for organizational part of risk management to know which activities and skills are required Does not address specific issues in risk management in this context ↓
ISO2700x (ISO 2013a)	ISO27005 provide guidelines for information security risk management Does not include specific risk analysis methods but does specify structured process from analysing risks to risk treatment plan	Extensive documentation about traditional risk management – good if no risk management exists or to improve but does not address current issues ↓
NIST Cyber Security Framework (NIST, 2014)	Risk-based cyber security framework Uses business drivers to guide cyber security activities and considering cyber security risks as part of the organization's risk management processes Framework implementation tiers provide context on how an organization views cyber security risk and the processes in place to manage that risk	Useful guidance to address cyber risk as part of the organization's risks management and get management attention ↑
NERC CIP Standards (NERC 2013)	No specific risks management content Reference to NIST "Risk Management Framework"	Non-compliance of NERC CIP Standards can help to address cyber risks as part of the organization's risk management →

5.1.4 Funding

How can actions support funding for information security improvements? How can CIE's be supported to prioritizing information security projects? The following Table 12 shows supporting parts of existing instruments.

Table 12: Funding instrument fulfillment

Instrument	Content	Authors assessment
CIP Guideline (FOCP 2014c)	Implementation is in the responsibility of CI provider respectively CI regulatory sector authorities A solidarity fund for cases of disruption should be organized by the government The community should adequately participate on the costs.	Does not depict how the CI providers will be monetary supported to invest in security ➔
COBIT5 for Information Security (ISACA 2012a)	Determine the availability and sources of funds (APO05.01) Information Security Budget: purpose of information security budget is to provide funding for information security programme	COBIT5 assists CIE in prioritizing of investments and make a proper budget to be prepared to get funds ➔
ISO2700x (ISO 2013a)	Does not provide information about funding or activities explicitly address funding	Does not depict how the CI providers will be monetary supported to invest in security 🡻
NIST Cyber Security Framework (NIST 2014)	Does not provide information about funding or activities explicitly address funding	Does not depict how the CI providers will be monetary supported to invest in security 🡻
NERC CIP Standards (NERC 2013)	Describes what actions have to be taken in which time frame but not how to fund them	Does not depict how the CI providers will be monetary supported to invest in security 🡻

5.1.5 Regulation

Which instruments define the need of regulations? How should regulation look like and how can regulation be audited? Table 13 shows supporting parts of existing instruments:

Table 13: Regulation instrument fulfillment

Instrument	Content	Authors assessment
CIP Guideline (FOCP 2014c)	It states that this guideline will not create new laws or regulations and should only be supportive to verify existing security infrastructure Implementation is in the responsibility of CI provider respectively CI regulatory sector authorities References to lists of relevant CI regulatory sector authorities and CI sector definition	Useful for further development of CIISM as this guideline includes definition and verification of CI security measurements; but no mandatory and cyber security specific actions or maturity levels ➔
COBIT5 for Information Security (ISACA 2012a)	Defines a set of management activities which can be used as standard requirements for CI providers	Does not show how to implement a regulatory framework nor define maturity levels or similar measurement actions ➔
ISO2700x (ISO 2013a)	Provides commonly used practises in information security management Existing certification and auditing procedures	Existing certification procedures Can be used as mandatory implementation guideline but does not deal with the importance of mandatory standards for information security ➔
NIST Cyber Security Framework (NIST 2014)	Defined categories with corresponding actions for cyber security Framework implementation tiers provide context on how an organization views cyber security risk and the processes in place to manage that risk	Can be used as starting point to define mandatory categories/actions and how to setup a maturity model Benchmarking of existing CI's Does not solve the problem of missing regulation ➔
NERC CIP Standards (NERC 2013)	Strict mandatory implementation dates for CIP Standards	Mandatory cyber security standards for US CI's Useful example / template for Swiss implementation ↑

5.1.6 Technology

Which instruments provide best practise guides? How can CIE be supported to protect old / weak designed ICS? Table 14 shows supporting parts of existing instruments.

Table 14: Technical Implementation instrument fulfillment

Instrument	Content	Authors assessment
CIP Guideline (FOCP 2014c)	No specific content for technology issues	Does not solve the problem of old / weak designed ICS nor addressing any technology issue ↓
COBIT5 for Information Security (ISACA 2012a)	Includes management activities to setup policies for malware prevention and connectivity security or managing the asset life cycle	Addresses several general topics on how to protect and secure assets but does not solve the problem of old / weak designed ICS →
ISO2700x (ISO 2013a)	ISO27001 (A.10 / A.11 / A.12) includes actions on how to implement operation and communication management, access controls as well procuration, development and maintenance of information systems	Can be used as template for minimum requirements but does not solve the problem of old / weak designed ICS and specific cyber risks →
NIST Cyber Security Framework (NIST 2014)	Protect section of the cyber security framework includes Access Control (PR.AC), Data Security (PR.DS), Maintenance (PR.MA) and Protective Technology (PR.PT) which address technology issues	Addresses several general topics on how to protect and secure assets Good starting point for standard requirements but does not solve the problem of old / weak designed ICS →
NERC CIP Standards (NERC 2013)	Standard CIP-007 specifies technical requirements against compromise cyber systems (including patch management, system hardening, user access management etc.)	Can be used as template for minimum requirements but does not solve the problem of old / weak designed ICS →

5.2 Enablers

This section elaborates on the definition of CIISM enablers for improving implementation, management and development of information security for CI's. The concept of enablers is introduced and explained using referencing instruments that supports implementation of CIISM enablers and further action to close gaps between current issues mentioned in section 4.3.

An enabler is build on five elements

1. Aim: Short description about the aim of the enabler
2. Dependencies: Describes on which other enablers or circumstances the enabler is dependent
3. Responsibilities: Who is in charge to take action for addressing the enabler
4. Referencing instruments: Which instruments (see section 3.3) define or address actions to reach the enabler goal
5. Gap: Which gaps exists between investigated instruments (see section 3.3) and the needed means to reach the enabler goal

Each of the six enablers (Figure 9) is described in a table by means of the five elements (see above) in the next sub chapters.

5.2.1 Awareness

Table 15: Enabler definition "Awareness"

Aim	Generate management attention and train employees to address IT risks adequately
Dependencies	IT risk awareness of the management is highly dependent on regulation and risk management enablers. If regulations set requirements i.e. for BCM or vulnerability management, the management is in charge to implement them and therefore get attention of the value of IT and which IT risks exists Training and education can improve the information security awareness of employees and stakeholders of CI's
Responsibility	CIE's
Referencing instruments	• COBIT5 for Information Security • NIST Cyber Security Framework
Gap	There is currently no gap of available instruments that supports awareness but there is a gap of internal processes and implementations for supporting actions that have to be addressed with mentioned dependent enablers

Information security get management attention often after an incident happens (Barzilay 2013). Awareness is useful for minimize risks or address specific information security risks to get attention. It is necessary to report every single incident of crucial ICT system to the management and illustrate the business benefit/impact by linking business services to these systems (NIST 2014).

COBIT5 (ISACA 2012a) and NIST (2014) can assist CI experts linking ICT risks with business drivers or identifying pain points to get management attention. This has to be individually implemented for each CIE. A mandatory implementation guideline for information security can improve the awareness of the management i.e. as certain non-compliance issues will rise up as risks on the top level management (Schneider 2014).

Supportive material and instruments to raise management and board members awareness for cyber risks:

- Informative brochure about current cyber risks and impact on CIE's
- Roadmap provided by FOCP on regulatory implementations

5.2.2 Cooperation / Education

Table 16: Enabler definition "Cooperation / Education"

Aim	Conveyance of national and international cooperation in the area of information sharing of incidents, knowledge and best practice implementation
Dependencies	Cooperation is dependent on the willingness of CIE to share information with same quality and therefore a regulation for information sharing and participation on security workshops can help to improve this situation
Responsibility	CIE's, FOCP
Referencing instruments	• CIP Guideline • CIP Strategy • MELANI • NERC CIP Standards • NIST Cyber Security Framework
Gap	There are organizations dealing with information sharing including members among others of CI sectors. There is requirement to join these groups and therefore no pressure to share information about past or current incidents

Cooperation needs effort and willingness of CI experts to share information and provide incident reports with other CIE's. NIST Cyber Security Framework (NIST 2014) describes incident report processes that can be used for national cooperation. MELANI (FOCP 2009a) or another governance organization should be established as central coordination and information spot. All CIE's should be part of this organization (FOCP 2014c). This would generate increased significance of the organization and provide an inter-sector knowledge sharing platform and best practice information to increase information security resilience of the whole CI environment.

Out of this organization, trainings and education of security experts and commonly used education material can be generated and shared among CIE's to lower costs and benefit from composite work. Education (Mühlheim 2014) should be promoted on each stage to increase the number of educated security personnel across all CIE's and therefore a benefit for Switzerland's community.

Tools/Documents that have to be provided by the responsible position:

- Process landscape including incident reporting and management
- Code of conduct for CI community
- International security trainings and certifications (i.e. CISSP (ISC2 2014), GICSP (GIAC 2014) etc.)

5.2.3 Cyber Risk Management

Table 17: Enabler definition "Cyber Risk Management"

Aim	Adjusted risk management for information security cyber risks
Dependencies	None
Responsibility	CIE's
Referencing instruments	• NIST Cyber Security Framework • CIP Guideline
Gap	Cyber risks management can be implemented with reference to NIST Cyber Security Framework and its supporting cyber risk activities but CIE's are in charge to change their way to identify and evaluate risks in their enterprise risk management

Risk management for cyber risk is highly volatile where fast changing cyber threats change risks landscape equally. Cyber risks (see section 3.1) have the characteristic that they are often classified as improbable – unless they happen recently (Barzilay 2013) and have an incalculable damage potential (World Economic Forum 2014). This fact differentiates cyber risks management from classic risks management where risks are classified by frequency of occurrence and degree of impact.

CIE's risk management have to address cyber risk by implementing a dynamic cyber risk management that includes risks beyond enterprise view. It is important to analyse risks not isolated from others but integrate cyber risks in a holistic CI risk management approach (see section 3.3.1). Risks landscape should be supervised by the regulatory sector authorities and should include especially not only enterprise but also risks for the whole community and economy. A chief information security officer (CISO) should be mandatory for a large enterprise and therefore regulated by the authorities. (Schneider 2014)

The following instruments can support regulations and have to be provided by FOCP, regulatory sector authorities or other CI organization:

- Cyber risk framework
- Common risks for CI's in terms of cyber risks and inter-sectorial view
- CISO Implementation Guideline

5.2.4 Funding

Table 18: Enabler definition "Funding"

Aim	CIE's should be able to provide information for governmental funding by providing needed reports
Dependencies	Funding is dependent on regulation as no governmental project will fund security investment if it is not a mandatory by the government Funding can be supported by CI cooperation's with a solidarity fund or similar activities
Responsibility	CIE's, FOCP and regulatory sector authorities
Referencing instruments	• CIP Guideline • CIP Strategy
Gap	Funding for information security is not mentioned in any investigated instrument. CI's as crucial services will not be able to invest in strong regulations if the dependent community is not willing to pay for it

Funding for information security implementations can help small and large CIE's to be able to fulfil and implement mandatory measurements to protect CI's in Switzerland adequately. Government and other CI organizations should provide funds or other financial means to assist CIE's on a monetary level. Further an implementation guideline or information platforms as well sponsored information security courses for information security experts can be funded by a national solidarity fund for CI's.

Shared risks have to be addressed in a shared context, as Switzerland's infrastructure and population benefits of a sustainable and protected CI. Therefore a solidarity fund for CI's supported by monetary means from taxes or other sources should be determined and applied in the near future.

Incentive system for well-protected CI's should be worked out by the FOCP and other organizations:

- Abatement of tax
- Better credit rating
- Decreased insurance fees

5.2.5 Regulation

Table 19: Enabler definition "Regulation"

Aim	Government provides a mandatory guideline for information security implementation of CIE's and setup a maturity model to classify and evaluate CIE's
Dependencies	Regulation is dependent on funding as mandatory regulation will raise costs on CIE's All other enablers can benefit of regulatory pressure to be implemented
Responsibility	Government, FOCP and regulatory sector authorities
Referencing instruments	• NERC CIP Standards • ISO 2700x • CIP Guideline
Gap	Only NERC CIP Standards provide a mandatory implementation guideline specific for CI's ISO2700x is well known and certification procedures are established but no specific implementation guideline exists for CI's and their needs

As CI's are crucial for Switzerland's population they should follow the same quality and security standards to fulfil the information security expectations. Regulation can be used to establish a common standard and maturity level for CI's. Regulatory authorities of corresponding CI sectors are in charge to categorize and review security maturity levels of each single CIE.

Mandatory regulation for information security measures implicates costs on the other side that has to be considered (Mühlheim 2014). It's supposable to define different maturity levels for different security zones. Where as an office zone does not have to fulfil highest security standards, a production control zone that is crucial for operating CI should be able to fulfil strongest security requirements (Mühlheim 2014).

Defined standards should be implemented in a predefined time frame to ensure a certain security level in short time (leaned on NERC CIP Standards (2013)).

Instruments that can support regulations are:

- New laws and regulation to take CIE's in charge
- NERC CIP Standards (as minimum standard for CI's information security)
- Maturity model (see section 10.3) to evaluate the level of maturity of CI's security implementations

5.2.6 Technology

Table 20: Enabler definition "Technology"

Aim	Implementation guideline for information security protection of CI's
Dependencies	Technology implementation guideline regulation can accelerate the degree of maturity and is therefore supportive to achieve a common CI minimum standard for information security implementation
Responsibility	CIE's, Government
Referencing instruments	• ISO 2700x • NERC CIP Standards • NIST Cyber Security Framework
Gap	Standards exist for different environments and requirements (see referencing documents) but legacy, as well new specific ICS are not designed for security requirements, which will not fulfil the requirements

Implementation guidelines for information security protection can improve current issues with legacy ICS in combination with educated security professionals (Assante 2014). Beside that, CIE and other organizations should apply pressure on ICS manufacturer to improve current and future systems to fulfil Switzerland's CI requirements (Anonymous 2014).

Implementation guideline will not include mandatory products or mechanism but will provide an additional best practise guide as supportive material that has to be adapted for sector specific needs.

Instruments that can support the technology enabler:

- High-level implementation guideline
- NER CIP Standards to align implementation guidelines
- Maturity levels to align implementation guidelines

5.3 Application

Application in this context means how this CIISM prototype can be used in practice and describes possible steps of implementation.

Governmental institution or regulatory sector authorities should initially promote CIISM. As regulation is one of the most referenced enabler, it is recommended to establish new regulations in a first step.

Further CIISM can be applied in different phases within a timeframe that has to be defined:

Phase 1: FOCP defines from the list of CI's (see section 10.2), which CIE have to fulfil the new regulations for CI's. Existing inventory of FOCP defines CI parts in detail. This is necessary to apply mandatory regulations. If not possible, CISSM can be used with best effort.

Phase 2: Baseline study for each relevant CIE will define current state of CIE's information security. Experts will investigate in the infrastructure to get important information about the current state of an infrastructure and its processes.

Phase 3: Minimum standard will be applied to all relevant CIE's. Based on the current state and the defined minimum standard the CIE has to close the gap or disclose them as risks in their risk assessment.

Phase 4: Defined maturity level will be reached by each CIE. Responsible sector authority will classify each part of the CI to maturity levels of CIISM. The CIE have to fulfil the maturity level for the corresponding parts of their infrastructure.

CIISM is only efficient if it is part of a holistic security management. As CIISM is very specific it does not completely but may be partially cover other parts of security i.e. physical security or job safety.

Beside that, a main challenge will be to achieve a balance between security requirements and business efficiency imperatives. Satisfying shareholders by maximizing company profits has often led to minimal security measures. (Hämmerli 2010, p.38)

5.4 Validation

The above-described CIISM is developed on the interpretation of inputs from CI experts and literature review. To validate these interpretations, CI experts were asked to comment and evaluate the CIISM prototype with the following evaluation form.

> **RO5**: Verification of explored discrepancies with CIE experts

5.4.1 Guideline

The following guideline (Table 21) was used where CI experts from the case study (see section 4.1) were asked to give a feedback about the CIISM prototype. The feedback was given between December 2014 and January 2015.

Table 21: CIISM prototype review questions

#	Question	Comment
1	Which important topics were not addressed in your opinion?	This question should give an impression of issues, which were not mentioned during the interviews of the case study or just raised during writing this paper
2	Which defined CIISM enabler is not relevant and in which order of importance would you arrange them?	This question should disclose if a CIISM enabler is completely useless or if one of the enablers outshines all others
3	What supportive material or instruments have to be provided to use CIISM?	Gives an impression of completeness of the mentioned instruments and tools
4	Which references to instruments and organizations are missing in the CIISM enabler references?	Gives an impression of completeness of the mentioned references
5	Free feedback on the literature research and CIISM prototype.	This question is asked to get inputs about the quality of the literature review and derivation of the enablers

Four feedbacks were returned in an appropriate timeframe. One requested feedback was not possible, as the expert has left the CIE in the period of writing this paper.

5.4.2 Feedback and Remarks

All requested CI experts do agree on the CIISM enablers in general. Some have different views on how current instruments can support the enablers or not. The feedback has than be integrated into the final CIISM prototype (see section 5.5).

The question of the order of importance of enablers was controversial discussed as some of the experts think "Regulation" is the most important enabler for CI information security and others think "Awareness", "Cyber Risk Management" and "Cooperation" are more important or all are important and there is no need for an order. That's the reason why no priority or sequence of the single enablers is defined.

Table 22 summarizes additional remarks on the CISSM enablers.

Table 22: Review remarks by CI experts

Enabler	Remarks
Awareness	None
Cooperation / Education	MELANI is currently verifying the list of members and will integrate missing CI providers (Wenger 2014)
Cyber Risk Management	Risk has to be acceptable from a community perspective and not from enterprise view where instruments like ISO27000 build on (Wenger 2014)
Funding	Funding does only work if awareness and regulation is properly implemented. Cost shifting to the consumer/customer must be discussed (Anonymous 2014)
Regulation	Regulatory authorities have to regulate by law that a CISO is needed in a larger company (compare data protection law) (Schneider 2014)
Technology	Difficulties will rise during the detail implementation phase as many CI's are different and the CIISM and referencing instruments does not describe in detail how to implement something Issues start often on the supplier side – IT soft- and hardware is often not developed sustainably (compare car industry). Liability of supplier on poor developed soft- and hardware has to be strengthened (Anonymous 2014)

As CI's are strategic attacking points as they are crucial for the whole economy and population, overlapping strategic functions of the government are important and necessary. Armed forces and intelligence services should be integrated in the national cyber defence strategy as the have the means and especially the connections to foreign services to act adequately before certain attacks happen (Mühlheim 2014). This point is therefore highlighted more prominent in the final prototype.

Additional instruments that are not considered in this paper but according to the interviewed CI experts can be helpful are:

- BSI
- ISO for BCM

5.5 Final CIISM prototype

The final CIISM (Figure 10) is the result from the preliminaries and the corresponding enablers validated by CI experts. It visualizes the influence of each enabler to fulfil the aim of CIISM. All enablers provide beneficial content to others and use output from other enablers to be efficient. The final prototype outlines especially that the government and its related departments of civil protection, armed forces and intelligence services are needed to coordinate overlapping and international topics and to provide adequate protection and know how to CIE's. According to Hämmerli (2010, p.34) "Effective protection also requires communication, coordination, and cooperation nationally and internationally among all stakeholders – industry, academia, the private sector, and government entities, including infrastructure protection and law enforcement agencies".

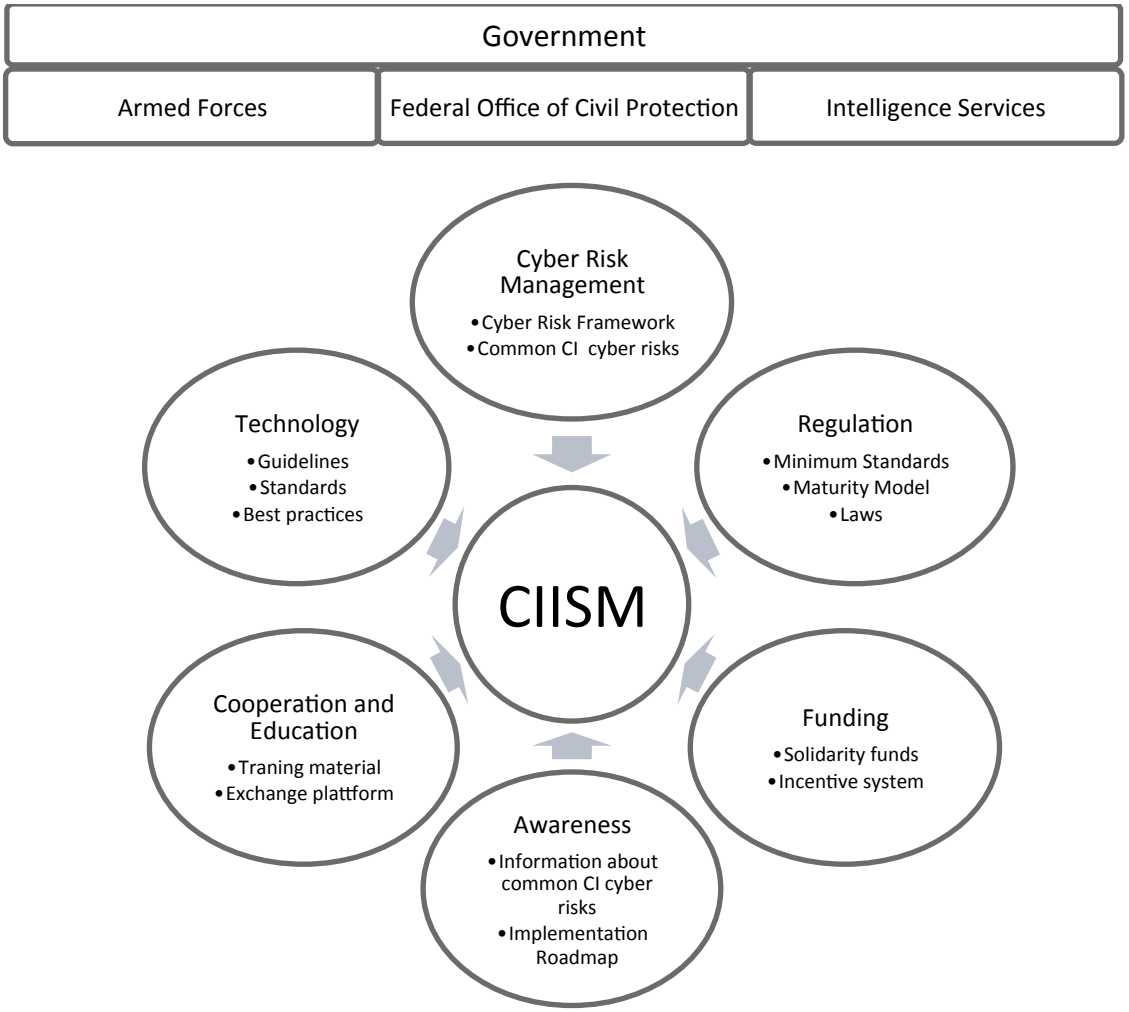

Figure 10: Final CIISM prototype

Table 23 summarizes the new elements of the final prototype (Figure 10) and the already described enablers in chapter 5.2.

Table 23: Final CIISM Elements

Element	Aim	Description
Government	Provide secure and stable CI services to the population	The legislator is in charge to set boundaries such as regulations and laws
Federal Office of Civil Protection	Responsible for monitoring implementations of CIISM in CIE's	Central coordination and monitoring is mandatory to guarantee the quality of CIISM implementation
Armed Forces	Generate and share cyber competences with CIE's	Armed forces may have to extend the budget for cyber defence and cyber warfare to current cyber risks. These special forces have then the means to build a powerful professional cyber defence which can share information and knowledge to CIE's
Intelligence Services	Support government and CIE's with information about international threat landscape, planned or ongoing attacks etc.	Intelligence services over the world can use existing information exchange platforms for cyber topics. As cyber threats do not stop at the border, it is a global topic.
Awareness	Generate management attention and train employees to address IT risks adequately	See section 5.2.1
Cooperation and Education	Conveyance of national and international cooperation in the area of information sharing of incidents, knowledge and best practice implementation	See section 5.2.2
Cyber Risk Management	Adjusted risk management for information security cyber risks	See section 5.2.3
Funding	CIE's should be able to provide information for governmental funding by providing needed reports	See section 5.2.4
Regulation	Government provides a mandatory guideline for information security implementation of CIE's and setup a maturity model to classify and evaluate CIE's	See section 5.2.5
Technology	Implementation guideline for information security protection of CI's	See section 5.2.6

CIISM must be an integral part of CIE's holistic security management and should not be implemented standalone. The basement of CIISM and other security models must be a common vision and strategy among CIE's and the government as well a strong political commitment to achieve the desired improvements (Hämmerli 2010, p.81). Vision, strategy and a holistic approach are essential foundations of an effective CIP.

6. CONCLUSION

Cyber threats are omnipresent not only for CI's. Outages, failures or manipulation through cyber threats can led to irreparable damage of information or information systems. Therefore these threats should not be underestimated.

This standardised prototype of information security model for CI's with focus on cyber risks acts as supportive instrument to improve current situation disclosed by CI experts. It builds on existing well-known instruments and can therefore be used also by other or related companies.

CI experts have disclosed weaknesses that were confirmed by literature. These weaknesses are named enablers in the CIISM prototype. The enablers guide the way to address current threat landscape adequately with existing instruments and new tools and regulation that have to be worked out first.

The enablers are:

- Awareness
- Cooperation / Education
- Cyber Risk Management
- Funding
- Regulation
- Technology

This CIISM prototype can be used on a volunteer base but experiences in the past of CI experts have shown that only mandatory instruments were widespread in the CI sector.

Current threats in ICT have en enormous potential of damage und CI's have to be protected with special attention. The government plays therefore an important role in releasing new laws and regulations as well monitor the implementation of the measures.

Education of experts and cooperation between involved stakeholders have to be supported also by the government to build a sustainable and effective organisation that is capable of the dynamic threat landscape.

Implementation of these enablers raises high costs. Nevertheless cyber risk management should outline the critical risks and measures have to be implemented forceful. In case of need, implementation should be forced by regulations. As the community benefit of a stable function of CI's, they should participate on the costs.

To conclude the interview's it was found out that many named problems in this paper are not new or already well known, but they get not the attention the situation supposed to. Cyber risks are not only for CI's a real threat – we all face these risks in our daily living. This paper should raise the awareness of cyber risks in our environment.

Based in this study further research have to be done to work out or adapted existing guidelines and frameworks mentioned in the enablers referencing instruments in section 5.2.

The attached approach of a CIISM maturity model (see section 10.3) can be used as starting point to build a prototype of a maturity model as an important tool to verify and mature the level of security in CIE's.

7. BIBLIOGRAPHY

Allan, K., 2013. Cyber-crime is greatest global threat to organizations' survival today. *http://www.ey.com*. Available at: http://www.ey.com/GL/en/Newsroom/News-releases/News_Cyber-crime-is-greatest-global-threat-to-organizations-survival-today.

Andress, J. & Winterfeld, S., 2011. *Cyber Warfare* first., Waltham: Elsevier.

Anonymous, 2014. Appendix: Interview Financial Institute.

Aquilina, A., 2014. Appendix: Interview Anna Aquilina.

Asprion, P.M., 2013. Assimilation of Compliance Software in Highly Regulated Industries: An Empirical Multitheoretical Investigation. *IEEE*, pp.3305–4414. Available at: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6480376&url=http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6480376.

Assange, J., 2006. WikiLeaks. Available at: https://wikileaks.org/? [Accessed May 5, 2014].

Assante, M., 2014. America's Critical Infrastructure Is Vulnerable To Cyber Attacks. *Forbes*. Available at: http://www.forbes.com/sites/realspin/2014/11/11/americas-critical-infrastructure-is-vulnerable-to-cyber-attacks/ [Accessed December 23, 2014].

Barandun, A., 2013. Schweizer Geheimniskrämerei hilft den Hackern. *Tagesanzeiger*. Available at: http://www.tagesanzeiger.ch/wirtschaft/Schweizer-Geheimniskraemerei-hilft-den-Hackern/story/29035539.

Barzilay, M., 2013. A simple definition of cybersecurity. *ISACA*. Available at: http://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?List=ef7cbc6d-9997-4b62-96a4-a36fb7e171af&ID=296.

Bucher, A. et al., 2009. Besserer Schutz für kritische Infrastrukturen. *Bevölkerungsschutz*, 5(November), p.24. Available at: www.bevoelkerungsschutz.ch.

Bundesministerium des Innern, 2009. *National Strategy for Critical Infrastructure Protection*, Berlin. Available at: http://www.kritis.bund.de/SharedDocs/Downloads/BBK/EN/CIP-Strategy.pdf;jsessionid=1E9991627588372512006811 5D8CA349.1_cid345?__blob=publicationFile.

Cohen, L., Manion, L. & Morrison, K., 2007. *Research Methods in Education* 6th ed., Oxon: Routledge.

DHS, Critical Infrastructure. *US Department of Homeland Security*. Available at: http://www.dhs.gov/critical-infrastructure [Accessed March 6, 2014a].

DHS, 2014. *Cybersecurity Capability Maturity Model*, Available at: http://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf.

DHS, What Is Critical Infrastructure? *US Department of Homeland Security*. Available at: http://www.dhs.gov/what-critical-infrastructure [Accessed March 10, 2014b].

Dictionary.com, 2014a. Education. Available at: http://dictionary.reference.com/browse/education [Accessed October 27, 2014].

Dictionary.com, 2014b. Regulation. Available at: http://dictionary.reference.com/browse/regulation [Accessed October 27, 2014].

Dictionary.com, 2014c. risk management. Available at: http://dictionary.reference.com/browse/risk management?s=t [Accessed October 27, 2014].

ENISIA, Critical Infrastructures and Services. *European Union Agency for Network and Information Security*. Available at: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services [Accessed March 12, 2014].

Europa, 2009. European critical infrastructures. Available at: http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/jl0013_en.htm.

Falliere, N., O Murchu, L. & Chien, E., 2011. Symantec Security Response. , 1.4(23.3.2013). Available at: http://securityresponse.symantec.com/en/id/content/en/us/enterprise/media/security_response /whitepapers/w32_stuxnet_dossier.pdf; 07/23/2013.

FinCEN, 2001. USA PATRIOT Act. *FinCEN*.

FOCP, 2014a. Aktuell. *Schutz Kritischer Infrastrukturen*. Available at: http://www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/themen/ski/aktuell.html [Accessed March 2, 2014].

FOCP, 2014b. Die Kritischen Infrastrukturen - Sektoren. *Bundesamt für Bevölkerungsschutz BABS*. Available at: http://www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/themen/ski/kritische_infrastrukturen.html#parsys_0001150 [Accessed March 1, 2014].

FOCP, 2007. *Erster Bericht an den Bundesrat zum Schutz Kritischer Infrastrukturen*,

FOCP, 2014c. *Leitfaden Schutz Kritischer Infrastrukturen*, Bern.

FOCP, 2012a. National strategy for the protection of Switzerland against cyber risks. , p.42.

FOCP, 2012b. *Nationale Strategie zum Schutz kritischer Infrastrukturen*, Available at: http://www.admin.ch/opc/de/federal-gazette/2012/7715.pdf.

FOCP, 2009a. The Federal Council's Basic Strategy for Critical Infrastructure Protection. , p.8. Available at: http://www.bevoelkerungsschutz.admin.ch/internet/bs/en/home/themen/ski/grundstrategie.parsysrelated1.78229.downloadList.33808.DownloadFile.tmp/grundstrategieen.pdf.

FOCP, 2009b. *The Swiss Programme on Critical Infrastructure Protection*, Bern.

GIAC, 2014. Global Industry Cyber Security Professional. Available at: http://www.giac.org/ [Accessed December 24, 2014].

Google, 2014a. Funding. Available at: https://www.google.ch/search?q=definition+funding [Accessed October 27, 2014].

Google, 2014b. Technology. Available at: https://www.google.ch/search?q=definition+technology [Accessed October 27, 2014].

Habegger, B. & Kmiecik, S., 2010. *Der Schutz kritischer Infrastrukturen: Gegenwart und Zukunft*, Zürich. Available at: http://www.bevoelkerungsschutz.admin.ch/internet/bs/en/home/themen/ski/publikationen_ski.parsys.33331.DownloadFile.tmp/schlussberichtexpertendialogskid.pdf.

Hämmerli, B., 2010. *Protecting Critical Infrastructure in the EU*, Brussels. Available at: http://www.ceps.eu/book/protecting-critical-infrastructure-eu.

Hevner, A.R. et al., 2004. *Design science in information systems research*, Tampa, FL 33620.

ISACA, 2012a. *COBIT5 for Information Security*, Rolling Meadows: ISACA.

ISACA, 2012b. *COBIT5 Framework*, Rolling Meadows: ISACA.

ISC2, 2014. CISSP Certified Information System Security Professional. Available at: www.isc2.org/cissp [Accessed December 24, 2014].

ISO, 2013a. An Introduction To ISO 27001 (ISO27001). Available at: http://www.27000.org/iso-27001.htm.

ISO, 2013b. Introduction To ISO 27002 (ISO27002). Available at: http://www.27000.org/iso-27002.htm [Accessed July 6, 2014].

Van Kessel, P. & Allan, K., 2013. Under cyber attack. *EY's Global Information Security Survey 2013*, (October). Available at: http://www.ey.com/GL/en/Services/Advisory/Cyber-security.

Kohlbacher, F., 2006. The Use of Qualitative Content Analysis in Case Study Research. *Forum: Qualitative Social Research*, 7. Available at: http://www.qualitative-research.net/index.php/fqs/article/view/75/153#g31.

Lange, E. & Kippels, D., 2009. Vernetzte Produktion ist ein lohnendes Ziel für "versierte" Industrie-Hacker. *INGENIEUR.de*. Available at: http://www.ingenieur.de/Themen/Datenschutz/Vernetzte-Produktion-lohnendes-Ziel-fuer-versierte-Industrie-Hacker.

Lehmann, A.P. & Kempe, F., 2014. Risk Nexus - Beyond data breaches : global interconnections of cyber risk. , (April), p.32. Available at: http://www.zurich.com/internet/main/SiteCollectionDocuments/insight/risk-nexus-april-2014-en.pdf.

Leimbach, T. et al., 2014. *Potential and Impacts of Cloud Computing Services and Social Network Websites*, Brussels.

Lütz, M., 2014. Appendix: Interview Mark Lütz.

MELANI, 2014. Information Assurance - Situation in Switzerland and internationally. *Semi-anual report 2014*, p.44.

MELANI, 2004. MELANI. Available at: http://www.melani.admin.ch/ [Accessed May 15, 2014].

MELANI, 2012. MELANI Newsletter. *admin.ch*. Available at: http://www.melani.admin.ch/dienstleistungen/archiv/01516/index.html?lang=de [Accessed May 15, 2014].

Mimoso, M., 2014. Patching Bash Vulnerability a Challenge for ICS, SCADA. *Threat Post*. Available at: http://threatpost.com/patching-bash-vulnerability-a-challenge-for-ics-scada/108575 [Accessed October 27, 2014].

Mingay, S., Spafford, G. & Wheeler, J.A., 2012. Updates in COBIT 5 Aim for Greater Relevance to Wider Business Audience. Available at: https://www.gartner.com/doc/1982323/updates-cobit--aim-greater [Accessed May 15, 2014].

Mühlheim, A., 2014. Appendix: Interview Andy Mühlheim.

NERC, 2013. CIP compliance. Available at: http://www.nerc.com/pa/CI/Comp/Pages/default.aspx [Accessed July 6, 2014].

NERC, 2009. Critical Cyber Asset Identification. Available at: http://online.wsj.com/public/resources/documents/CIP-002-Identification-Letter-040609.pdf.

NIST, 2014. Framework for Improving Critical Infrastructure Cybersecurity. Available at: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

NIST, 2006. *Glossary of Key Information Security Terms*, Available at: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=913810.

NZZ, 2008. Stromausfall in Zürich Nord. *NZZ*. Available at: http://www.nzz.ch/aktuell/startseite/stromausfall-zuerich-1.814906.

OECD, 2011. OECD Stats. Available at: http://stats.oecd.org.

Perkins, E., 2012. Enough Already with the Critical Infrastructure Security Whining! *Gartner Blog*. Available at: http://blogs.gartner.com/earl-perkins/2012/08/31/enough-already-with-the-critical-infrastructure-security-whining/.

Perkins, E., 2014. NIST Framework Establishes Risk Basics for Critical Infrastructure. , p.4. Available at: https://www.gartner.com/doc/2667132/nist-framework-establishes-risk-basics.

Perkins, E., 2013. The Impact of Critical Infrastructure Protection Standards on Security. Available at: https://www.gartner.com/doc/2367918/impact-critical-infrastructure-protection-standards.

Pettey, C. & Goasduff, L., 2010. *Gartner Reveals Top Predictions for IT Organizations and Users for 2011 and Beyond*, Stamford. Available at: http://www.gartner.com/newsroom/id/1480514 [Accessed March 11, 2014].

Ray, W.J., 2014. *Evolutionary Psychology: Neuroscience Perspectives concerning Human Behavior and Experience* 1st ed., Just The facts101.

Rid, T., 2013. So why aren't hackers crashing the grid. *Foreignpolicy.com*. Available at: http://www.foreignpolicy.com/articles/2013/07/23/cyber_sabotage_is_easy_i_know_i_did_it [Accessed May 6, 2014].

Rivera, J., 2013. *Gartner Reveals Top Predictions for IT Organizations and Users for 2014 and Beyond*, Orlando. Available at: http://www.gartner.com/newsroom/id/2603215.

Saunders, M., Lewis, P. & Thornhill, A., 2009. *Research Methods for Business Students* 5th ed., Essex: Pearson Education Limited.

SBB, 2005. *SBB Verwaltungsrat verabschiedet Bericht zur Strompanne*, Available at: http://m.sbb.ch/news.newsdetail.2005-8-28312.html.

Schneider, A., 2014. Appendix: Interview Andreas Schneider.

Snowden, E., 2013. Eight things we learned. *The Guardian*. Available at: http://www.theguardian.com/world/2013/jun/18/edward-snowden-live-q-and-a-eight-things.

Stürmer, M., 2013. Ohne Strom wäre unser Leben arm, brutal, bösartig. *Die Welt*. Available at: http://www.welt.de/debatte/kommentare/article119543993/Ohne-Strom-waere-unser-Leben-arm-brutal-boesartig.html.

Trochim, W. & Donnelly, J.P., 2006. *Deduction & Induction*, Atomic Dog. Available at: http://www.socialresearchmethods.net/kb/dedind.php [Accessed March 25, 2014].

VDE, 2006. Strompanne der SBB vom 22. Juni 2005. *VDE*. Available at: http://www.vde.com/de/fg/ETG/Archiv/Publikationen/Rundbriefe/2006-Exklusiv/2006-01/Technik-Trends/2006-exklusiv/Seiten/strompanne.aspx [Accessed April 4, 2014].

De Villiers, M.R. (Ruth), 2005. *Interpretive Research Models for Informatics: Action Research, Grounded Theory, and the Family of Design- and Development Research*,

Wenger, N., 2014. Appendix: Interview Nick Wenger.

World Economic Forum, 2014. *Global Risks Report* 9th ed., Available at: http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf.

Yin, R.K., 2009. *Case Study Research: Design and Methods* 4th ed., California: SAGE.

Zucker, D., 2009. *How to Do Case Study Research*, Available at: http://scholarworks.umass.edu/cgi/viewcontent.cgi?article=1001&context=nursing_faculty_pubs.

8. ABRREVIATIONS

Table 24: Glossary of Terms

Term	Description
BASEL I/II	Basel Accords; recommendations on banking laws and regulations issued by the Basel Committee on Banking Supervision
BCM	Business Continuity Management
BSI	Bundesamt für Sicherheit in der Informationstechnik (Deutschland) (German Federal Office for Information Technology)
BYOD	Bring Your Own Device
CI	Critical Infrastructure
CIE	Critical Infrastructure Enterprise
CIISM	Critical Infrastructure Information Security Model
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CISO	Chief Information Security Officer
CISSP	Certified Information System Security Professional
COBIT	Control Objectives for Information and Related Technology
CSF	Cyber Security Framework
CSIRT	Computer Security Incident Response Team
DDOS	Distributed Denial of Service
EBU	European Broadcast Union
FINMA	Eidgenössische Finanzmarktaufsicht Schweiz (Swiss Financial Market Supervisory Authority)
FOCOM	Federal Office of Communication
FOCP	Federal Office of Civil Protection
GICSP	Global Industrial Cyber Security Professional
ICS	Industrial Control Systems
ICT	Information and Communication Technology
ISACA	Information Systems Audit and Control Association
ISMS	Information Security Management Systems
ISO	International Organization for Standardization
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NSA	National Security Agency (United States of America)
MELANI	Melde- und Analysestelle Informationssicherung
OECD	Organisation for Economic Co-operation and Development
PCI DSS	Payment Card Industry Data Security Standard
SCADA	Supervisory Control and Data Acquisition
SCM	Service Continuity Management
SKI	Schutz Kritischer Infrastrukturen (Critical Infrastructure Protection)

9. LIST OF FIGURES / TABLES

9.1 Figures

9.2 Tables

10. APPENDIX

10.1 Interviews

Following guided interviews with CI experts in the area of Risk, Information Security and IT Security have been hold as a primary research source. Interviews were executed in the period from April to July 2014. The interviews were digitally recorded and later transcribed. The interview partners (except the partner from a national financial institute) allowed disclosing their name and company.

The list of interviews is ordered by execution date and has no further meaning.

10.1.1 Nick Wenger, BABS

- Name: Nick Wenger
- Firma: Bundesamt für Bevölkerungsschutz
- Position: Projektleiter Schutz kritischer Infrastrukturen

1. Was unternimmt der Bund für den Schutz kritischer Infrastrukturen? Was ist das Ziel des Projektes Schutz kritischer Infrastrukturen

Aufgabe: Koordinationsfunktion - Zusammenarbeit mit Fachbehörden und Betreibern
Ziel: Widerstandsfähigkeit der Schweiz in Bezug auf kritische Infrastrukturen verbessern. Verhindern von großflächigen Ausfällen bzw. minimieren des Schadenausmasses. Möglichst rasch wieder die Funktionsfähigkeit aufnehmen und/oder die Bevölkerung im Notfall zu unterstützen.
Outcomes:

1. Nationale Strategie zum Schutz kritischer Infrastruktur: Vom Bundesrat im Juni 2012 verabschiedet. 15 Massnahmen definiert (14 davon für die Verbesserung der Koordination und Unterstützung im Ereignisfall, 1 zur Verbesserung der Widerstandsfähigkeit der kritischen Infrastrukturen. Strategie eng zusammenhängend mit der Cyber Strategy des Bundes erarbeitet.
2. Inventar SKI (Brücken, Strassen, Einrichtungen wie Datacenter usw. welche für das funktionieren der Schweiz relevant sind)
3. Informations- und Sensibilisierungsprodukte für die Bevölkerung
4. Leitfaden Schutz kritischer Infrastruktur (sozusagen ein Framework für Massnahme 15 der Strategie).
   a. Kein Gesetz. Ist eine Absichtserklärung und somit nicht bindend für eine Unternehmung
   b. Kombiniert BCM und Risiko Managementansätze
   c. Arbeitsgruppen sämtlicher Bundesbehörden mit Verantwortung in diesem Bereich sowie Vertretern von betroffenen Firmen sind konsultiert worden

d. Hilfsmittel auf freiwilliger Basis → Regulierungsbehörden könnten diesen dann anwenden oder als verpflichtend definieren, ist aber nicht in der Hohheit des BABS

Finanzielle Entschädigung für Schutzmassnahmen:

bestehende Mechanismen über den politischen Weg existieren:

- Etablierte Finanzierungsmechanismen (z.B. Schienenverkehr), Leistungsaufträge (SRG) usw.
- Politische Unterstützung muss vorhanden sein, damit entsprechendes Budget für diese Vorhaben gesprochen werden. Dies muss über die bestehenden politischen Bestrebungen geschehen, es wird kein Geldtopf auf Bundesebene nur für die Sicherheit aller Infrastrukturen geben. Dies muss in den einzelnen Bereichen gesprochen werden.
- Es wird kein zentraler Bundespot geben, welcher Gelder zur Verfügung stellt
- Versicherungen: Prämienentschädigung für entsprechenden Schutz der Infrastruktur
- (Input M.Schlüter:) Z.B. könnte man ein Maturity Level-basiertes Framework verwenden aufgrund welcher Stufe man sich eine entsprechende Prämienverbilligung einhandeln könnte.

Wenn man mit Anreizen arbeitet, ist die weitflächige Umsetzung einer Vorgabe auf freiwilliger Basis einfacher als wenn man auf gesamtschweizerischer Ebene für alle Unternehmung ein Gesetz definiert und dieses durchsetzen möchte

2. Was unternimmt der Bund im Bezug auf Regulatorien / Vorschriften für den Schutz kritischer Infrastrukturen? Vertraut man auf die Selbstregulierung des Marktes?

- Es gibt viele Instrumente und Standards. Aber decken diese genau die Anforderungen an kritische Infrastrukturen ab? Man muss aufpassen, dass man sich nicht in Details verliert und dabei das Big Picture der Risiken mit allen Zusammenhängen der kritischen Infrastrukturen übersieht.
- Enge Zusammenarbeit mit den Regulierungs- und Aufsichtsbehörden der verschiedenen Branchen / Sektoren
- Keine Verpflichtung für die Firmen, da es keine gesetzliche Grundlage gibt. Es wird auch nicht angestrebt, dies in der nächsten Zeit zu ändern. Zuständige Stellen sollen entsprechende angepasste Regulatorien für ihren Bereich definieren und umsetzen

Welche Regulierungs- und Aufsichtsbehörden gibt es in den Sektoren? (z.b FINMA,..)

- Finanzbereich FINMA; SNB
- Energiebereich: ElCom; BFE
- Telekommunikationsbereich: ComCom, BAKOM

Blackout durch Vernetzbarkeit auch durch Ausfälle im Ausland / Nachbarländer z.B. Kein Nationales IT Gesetz notwendig. Energiebehörde muss Strom liefern und somit auch ihre IT sicherstellen (Regulationsverantwortung BFE/ElCom)

3. Was sehen Sie als die grösste Herausforderung um den Schutz (im speziellen die Information Sicherheit) sicherzustellen?

Schutz der zwei wichtigsten Versorger der Bevölkerung:

- Stromversorgung
- Telekommunikation

Sind die größten und wichtigsten Infrastrukturen da praktisch alle Unternehmen und ein Großteil der Bevölkerung sehr stark von der Stromversorgung oder der Telekommunikation abhängig sind.
Finanzierung: Nicht alle Bereiche sind auf dem gleichen Stand und viele Mechanismen existieren auch schon. Sicherheit ist nichts Neues und nicht jedes Element einer Unternehmung benötigt die selbe Stufe von Sicherheit. Zudem muss man differenzieren zwischen relevanten und notwendigen Bereichen welche besonders geschützt werden müssen.
Problem ist sicherlich auch die Digitalisierung welche aus wirtschaftlicher Sicht durchaus Sinn machen, aber dadurch neue Risiken und Abhängigkeiten entstehen. Man macht sich zu wenig Gedanken, wie man in einer Situation ohne IT Mittel den Betrieb aufrecht erhalten könnte.

4. Wie schützt sich der Bund (die Bundesstellen/Ämter) selbst? Gibt es interne Vorschriften z.B. gewisse ISO Standards zu erfüllen um die Informationssicherheit zu gewährleisten?

Das VBS hat seine Vorschriften und internen Regelungen
Vorschriften/Auflagen sind sehr streng da es auch um militärischen Systeme geht
Man ist versucht die Sicherheit so zu leben wie man es von Anderen fordert
ISO2700x ist ein Begriff und wird verfolgt
Risikoschulung für alle Mitarbeiter (Stufengerecht)

5. Verfolgt man die Entwicklungen in anderen Ländern wie z.b. Deutschland KRITIS oder in den USA das Projekt Critical Infrastructure Protection und die damit verbundenen Frameworks wie Cybersecurity Framework?

- EU: Programm für den Schutz kritischer Infrastrukturen: EPCIP
- Engere Zusammenarbeit mit Frankreich, Deutschland und Österreich
- Österreich: CD herausgegeben wo man testen kann wie sicher ist man / grosse Unterstützung von Regierungsebene ist wichtig und zeigt Wirkung / Führungskräfte wurden ins Kanzleramt eingeladen etc.
- GB und Holland sind sehr weit in diesem Bereich von CIP Strategien
- Bei der Ausarbeitung von Modellen oder Leitfaden profitiert man von bestehenden Arbeiten auch aus dem Ausland. Auch die positiven und negativen Erfahrungen fliessen in diese Arbeiten ein
- SKI ist politisch nicht sehr hoch angesiedelt. Cyber Strategy ist prominenter vertreten und wird häufiger in den Medien diskutiert

6. Wie stehen Sie einer übergreifenden Regulierung und Einhaltung spezieller Frameworks für kritische Infrastrukturen gegenüber? Wo könnte sich Wiederstand breit machen bzw. was könnten die Hürden sein, welche man nehmen müsste?

- Übergreifender Framework ja (Leitfaden); übergreifende Regulierung nicht notwendig. Verantwortung zur Durchsetzung des Frameworks liegt bei den jeweiligen Aufsichts- und Regulationsbehörden.
- Kosten wären ein wichtiger Punkt. Wer übernimmt die Kosten wenn man etwas auf Bundesebene vorschreibt?

- Übergreifendes gesamthaftes Framework für alle Bereiche, welches in die Tiefe geht, wird in der Schweiz nicht möglich sein da die Umgebungen zu unterschiedlich sind. Dafür sind die zuständigen Fachbehörden zuständig welche diese Regelungen (evtl. auf Basis der Empfehlung des Bundes und der ausgearbeiteten Frameworks) festlegen
- Großes Interesse der betroffenen Firmen und Fachbehörden ist vorhanden und die Zusammenarbeit in diesem Bereich ist sehr gut
- Gewisse Fachbehörden haben schon starke Regulierungen und könnten gegenüber neuen Regulierungen skeptisch sein. Es sollte auf einer unterstützenden Basis aufbauen wobei die Fachbehörden die Regelungen selber definieren und durchsetzen können
- Fachbehörden sind unabhängig vom Bund aber eingegliedert in die Prozesse (z.B. Energie, Finanz oder Telekommunikationsbereich)
- Man muss differenzieren zwischen rein firmenbezogener Risiken und Risiken welche für das gesamte System relevant sind
- Branchen erlassen auf ihrer Ebene über die Branchengesetze oder die Regulierungsbehörde die Vorschriften und Regeln. Z.B. jetzt wird das Stromgesetz überarbeitet und es wird festgehalten, dass die kritischen Komponenten für die Stromversorgung auch die IT umfasst und somit diese einen speziellen Schutz geniesst

7. Alternative, an welchen Punkten müsste man ansetzen, um die Awareness und Readiness for neuen Cyber Threats zu schaffen?

Ausfälle und negative Ereignisse zeigen die Lücken und Notwendigkeit am ehesten auf
Es darf aber kein Alarmismus gelebt werden, wir sind nicht in einem dauernden Kriegszustand
Ausfälle bieten ein „Window of opportunity“ welches man nutzen kann um die Risiken aufzuzeigen und Maßnahmen zu ergreifen
Wichtig: man muss präzise sein in der Awareness und genau darauf Hinweisen was die Auswirkung ist. Sind es „nur“ Kundendaten welche verloren gehen oder ist der Betrieb von gesamt gesellschaftlicher Bedeutung gefährdet?

10.1.2 Anonymous, Financial Institute

- Name: <anonymisiert>
- Firma: <anonymisiert> nationales Finanzinstitut
- Position: Operational Security

1. Was macht ihre Unternehmung zu einem Teil der kritischen Infrastrukturen?

- **Zählen Sie die Unternehmung als Teil der kritischen Infrastrukturen der Schweiz?**

  - Ja, der Finanzsektor zählt auch dazu
  - Wir sehen uns auch als Teil der kritischen Finanzinfrastrukturen
  - Auch deswegen sind wir bei MELANI des Bundes eingebunden

- **Was sind die wichtigsten Assets der Unternehmung?**

  Ohne IT funktioniert die Bank gar nicht
  Die Daten sind sehr wichtig. Jedoch funktionieren die Daten nur, wenn die IT funktioniert
  - Daten
  - IT infrastruktur

- **Was wird als grösster Risikofaktor angeschaut? Was wäre ein GAU?**

  BCM Strategy deklariert: Total Ausfall IT/Daten

2. Welche Angriffe auf (Information) Assets der Unternehmung gab es in den letzten 10 Jahren?

- **Gab es in den letzten 10 Jahren einen grösseren Zwischenfall in Bezug auf Informationssicherheitsverletzung?**

  - IT ist groß und aufgrund von Business Anforderungen gibt es viele Changes womit die Wahrscheinlichkeit steigt, dass ein gravierender Fehler geschieht
  - Fehler aufgrund von Changes lösten bisher 2x die IT-Notfallorganisation aus. Dies geschieht nur bei einer sehr kritischen Situation
  - Erfolgreiche Angriffe von Außen sind uns keine bekannt. Die Angriffe, die wir sehen, richten sich mehr auf den Kunden selber (schwächstes Glied)

3. Wie entgegnen Sie Gefahren im Information Security Bereich?

- **Gibt es ein Risk Management / Wem ist es unterstellt?**

  - Ja es gibt ein Risk Management
  - Anhand eines Framework werden diese Risiken geführt
  - Die IT hat ihre Risk Szenarien, Risiken welche klassifiziert werden
  - Als ein hohes Risiko wird z.B. der Malwarebefall eingeschätzt (in Richtung Sabotage welche den Betrieb behindert bzw. Daten beschädigt)
  - Operational Risk ist ein etwas neueres Thema und gibt es seit ca. 10 Jahren

- **Ist die IT ein essentieller (Risiko-) Faktor der Unternehmung?**

  Ja die IT ist der kritische Teil der Infrastruktur und somit auch ein Risiko Faktor für die gesamte Unternehmung. Der Totalausfall IT/Daten gilt als das WorstCase Szenario für die Bank.

- **Was wird unternommen, um diesen Risiken entgegen zu wirken?**

  - Die meisten der Top-Risiken sind über die BCM-Strategie und dem dazugehörigen IT SCM adressiert
  - Vor Cyber Risiken schütz man sich durch Massnahmen im Perimeter, Arbeitsplatz, etc.
  - Maleware Befall ist ein grosses Thema, grösste Cyber Gefahr da Malware trotz aller Massanahmen weiterhin einschleusbar bleibt → u.a wurde deswegen der Browser mit welchem im Internet gesurft wird, vermehrt isoliert
  - Zu den Top Risiken zählt die Datenwiederherstellung im Gesamtkontext nach einem Totalausfall. Einzelne Restores können getestet werden, aber das

Zusammenspiel nach einem Totalausfall birgt die grössten Risiken (passen die Daten wieder zusammen?)
- Monitoring von Angriffen könnte verbessert werden
- Organisatorisch ist man gut aufgestellt
- Im Rahmen der BCM Strategy werden die Risiken ausgewiesen
- Zudem hat die Bank hat ihr eigenes Notstromnetzwerk welches im Notfall genutzt wird (Um Abhängigkeit von Stromanbietern zu reduzieren)

- **Gab es Cyber Angriffe jeglicher Art? Schützt man sich speziell?**

  - Keine bekannten Angriffe auf die Unternehmung selber, der Kunde steht im Vordergrund
  - Viren und Maleware Befall im kleinerem Rahmen (durch das surfen im Web)
  - Risiken sind bekannt und die Management Attention ist vorhanden

- **Wie haben sich die Ausgaben zum Schutz der Informationssicherheit im Anbetracht von Cyber Crime verändert?**

  - Operativ macht man sicher mehr
  - CERT (Computer Emergency Response Team) wurde aufgestellt
  - Sicherheits-Roadmap besteht und entsprechend Mehrbedarf an Finanzen ausgewiesen

- **Ist MELANI ein Begriff? In welchem Zusammenhang?**

  - Ja dieses Finanzinstitut ist bei MELANI eingebunden
  - Nachteil ist es, dass MELANI Best Effort ist / Treffen sind sehr frontal da die Anzahl Teilnehmer zu gross ist. Keine Diskussionen im kleinen Rahmen
  - MELANI unterstützt aktiv bei Vorfällen. Haben da gute Erfahrungen gemacht
  - Der Austausch von Schwachstellen Informationen oder über Angriffe ist eine Vertrauenssache und man muss sich die Frage stellen, wem möchte man diese Informationen anvertrauen.
  - Was muss der Bund bereitstellen? Was muss MELANI bieten? Dies wechselt über die Jahre immer wieder etwas. Der technische Bereich bei MELANI wandelt sich, auch durch die Cyber Strategy des Bundes.

4. Welche Vorschriften oder Standards müssen/werden von ihrer Unternehmung im Bereich Information Security verfolgt

- **Welche Compliance Anforderungen (SOX, Basel II/III etc.) müssen erfüllt werden und aus welchem Grund?**

  - FINMA Vorgaben: z.B. Rundschreiben zu operational Risk (Anhang 3) umsetzen bis 2015
    Anforderungen an Information Sicherheit, an den Schutz von Daten
  - ISO27002; wird nicht vorgegeben, wird aber intern verfolgt
  - Bankengesetz (Bankkundengeheimnis etc.)
  - OR
  - Basel2/3: hat direkten Zusammenhang mit Operational Risk. Je weniger Risk man nimmt, desto weniger Eigenkapital benötigt man
  - SOX betrifft dieses Finanzinstitute nicht

- **Werden Compliance Management Systeme eingesetzt?**
- **Gibt es andere Instrumente und Standards (Frameworks, Applications etc.) welche der Unternehmung helfen, Risiken zu minimieren/verwalten?**

  Ja. ITIL, COBIT, IS0 27000 Reihe sind im Einsatz
  Zur Zeit werden Vulnerability Scans nur beschränkt genutzt. Ist aber ein Thema auf der erwähnten Sicherheits-Roadmap.

- **Gibt es Bereiche welche ihrer Meinung nach zu wenig durch solche Frameworks / Tools unterstützt werden?**

  Meiner Meinung nach sind die Frameworks relativ komplett. Dies sind sie auch, weil sie eher generisch gehalten sind. Somit liegt die Herausforderung weniger bei den Frameworks sondern bei deren Umsetzung, resp. der konkreten Interpretierung/Übersetzung für die eigene Firma.

- **Was empfinden Sie als Vor- und was als Nachteil von Compliance Vorschriften?**

  Helfen natürlich zur Verbesserung zum Schutz der Infrastrukturen bzw. üben Druck auf das Management aus diese Risiken zu definieren und entsprechende Massnahmen zu initiieren
    - Interne und vor allem externe Revisoren tragen ihren Teil dazu bei, dass der Druck auf das Management wirkt.

5. Würde ein branchenübergreifendes Information Security Compliance Framework mit vorgeschriebenen Audits mehr Sicherheit bringen?

- **Wie stehen Sie einem umfassenden Framework zur Erfüllung von Compliance Anforderungen für kritische Infrastrukturen in der Schweiz gegenüber? Was könnten mögliche Hindernisse sein? Wie wäre die Akzeptanz in den betroffenen Betrieben?**

  Kritischer Sektor ist sicherlich der Stromsektor
  Abhängigkeit von Strom ist sehr gross
  Wie schützen sich diese vor Angriffen? Befinden sich oft in einer grauen Ecke was die Regulationen anbelangt. Wie werden die Industriesysteme geschützt welche in diesem Bereich sehr verbreitet sind? Diese sind nicht robust und nicht Angriffe von Aussen geschützt. Trotzdem werden diese auch mit dem Internet verbunden.

  Es wäre sicherlich hilfreich, wenn es übergreifend etwas für alle geben würde. Minimalanforderungen erfüllt werden.
  Die Frage ist, wo stehen die anderen Sektoren? Problem sind dann vermutlich die Kosten für die Implementation. BCM ist sehr anspruchsvoll und kostet viel.
  Man kann somit nicht zu streng sein. Aber es gibt auch heute schon Best Practice.
  Hersteller müssten ebenfalls in die Pflicht genommen werden. Z.B. müssten Industriesteuerungen sicherheitstechnisch robuster werden.
  Cyber Strategy vom Bund ist ebenfalls im Aufbau, wie viel diese verändern wird ist noch offen.

6. Was ist die grösste Herausforderung in der Informationssicherheit für die nächsten 5 Jahre?

Wenn man über Informationssicherheit spricht, fallen oft die Begriffe
- Vertraulichkeit
- Integrität

Wobei die Verfügbarkeit des öftern vergessen geht!

Vertraulichkeit kann abhanden kommen, aber die Bank kann noch weiter operieren
Verfügbarkeit: wird diese mittels einer breitflächigen Attacke auf die Daten / Infrastruktur angegriffen, dann ist es schwierig wieder up and running zu sein.
Sind die Daten noch erhalten aber inhaltlich kaputt, so stellt dies ebenfalls ein Problem dar.
Gefahr ist intern erkannt, aber es wird noch Jahre dauern bis man mit diese Probleme vollumfänglich beherrschen wird.

Wenn der Angreifer etwas Geld aufwendet dann stehen die Change gut, dass man an Informationen kommt
Verfügbarkeit und Cyber Threats sind auf der Roadmap Informationssicherheit

10.1.3 Andreas Schneider, SRG SSR

- Name: Andreas Schneider
- Firma: SRG SSR
- Position: Fachführung IT Sicherheit Technik und Informatik

1. Was macht ihre Unternehmung zu einem Teil der kritischen Infrastrukturen?

- **Zählen Sie die Unternehmung als Teil der kritischen Infrastrukturen der Schweiz?**

  - Die SRG SSR ist durch den Bund definiert als Teil der kritischen Infrastrukturen der Schweiz
  - Die SRG SSR hat den kritischen Auftrag, die Bevölkerung im Notfall zu informieren
  - Teil der Definition der kritischen Infrastrukturen durch den Bund → Verweis auf die SKI Dokumentation (Bereich Telekommunikation / Kommunikation →Medien) des Bundes (http://www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/themen/ski/kritische_infrastrukturen.html)
  - Die SRG SSR ist somit auch Bestandteil der Inventarliste des Bundes von kritischer Systeme (befindet sich noch im Aufbau)

- **Was sind die wichtigsten Assets der Unternehmung?**

  - Distributionskanäle / Infrastruktur der ersten Kanäle:
    - Die Radio Infrastruktur, speziell die ersten Kanäle (über UKW/DAB+ etc.) sind essentiell
    - Diese müssen immer zur Verfügung stehen (ansonsten müsste die Aufgabe der Information der Bevölkerung von den Blaulichtorganisationen wie der örtlichen Polizei übernommen werden) damit der Bund sich aufschalten und Informationen an die Bevölkerung richten kann

→ Beispiel: Szenario Erdbeben in Basel (Modellberechnungen basieren auf diesem Ereignis aus dem Jahre 1356 und ist hier beschrieben: http://www.seismo.ethz.ch/eq_swiss/Szenario/index)

- Nicht kritisch in diesem Zusammenhang sind die Produktionssysteme zur Produktion von Sendungen und Nachrichten
- MPLS Backbone der IT Infrastruktur muss aber auch als senderelevant angeschaut werden. Im Falle eines Ausfalls wären die Informationskanäle ebenfalls betroffen und stark eingeschränkt

- **Was sind die am meisten zu schützenden Werte (Informationen, Gegenstände, Immobilien etc.):**

  - Distributionsinfrastruktur der Informationskanäle (primäre Radiokanäle)
  - IT Infrastruktur (Immer mehr Sendesysteme haben ein IT Interface)

- **Was wird als grösster Risikofaktor angeschaut / was wäre der GAU?**

  Erstes Szenario: Nicht in der Lage zu sein, die Bevölkerung zu informieren
  Eine Attacke auf die SRG Infrastruktur könnte die SRG bzw. den Bund daran hindern, notwendige Informationen an die Bevölkerung zu richten
  z.B. Bei einem Stromausfall in gewissen Teilen der Schweiz macht die SRG zum einzigen Instrument für die Informationsverbreitung. In der Kette der kritischen Infrastrukturen ist die SRG relevant, wenn andere kritische Infrastrukturen Ausfallen

  Zweites Szenario: Falschinformationen werden gezielt über die SRG Informationskanäle an die Bevölkerung verbreitet
  Hackerangriff mit dem Ziel, Unruhe oder Panik zu generieren
  Dies wirkt sich dann auf alle anderen Ebenen auch von kritischen Infrastrukturen aus

2. Welche Angriffe auf (Information) Assets der Unternehmung gab es in den letzten 10 Jahren?

- **Gab es in den letzten 10 Jahren einen grösseren Zwischenfall in Bezug auf Informationssicherheitsverletzung?**

  - Generell: Man ist immer Angreifbar; es findet eine zunehmende Digitalisierung der gesamten Medientechnik statt; Radiosysteme sind auf klassischen IT Systemen installiert
  - Vergangene Angriffsszenarien basierten auf krimineller Energie um z.B. Geld von Bankkonten zur eigenen Bereicherung zu entwenden
  - Mediensysteme waren einzelne Silos und somit weniger über das Internet angreifbar
  - Heutiges Angriffsszenario ist ideologisch getrieben; Systeme sind vermehrt vernetzt und sind mit dem Internet verbunden; keine einzelnen Silos mehr
    - Die Medien und insbesondere die SRG ist ein Sprachrohr des Staates (der neutralen Schweiz)
    - Aussagen über Länder wie China oder Syrien können ein Angriffspunkte für staatliche / halbstaatliche Cyber Aktivisten/Armeen sein, welche aufgrund negativer Berichterstattung (aus der Sicht der Betroffenen Länder/Regierungen) eingreifen und ein bestimmtes Ziel verfolgen

        - Mediensysteme sind nicht mehr getrennt von der IT, sondern sind Teil davon; früher war dies nicht der Fall
    - Angriffswahrscheinlichkeit steigt und die Auswirkungen nehmen ebenfalls zu
    - Ein Anstieg von Angriffen ist erkennbar
        - Gezielte Angriffe auf Journalisten mit Malware (Angreifer kennen die Arbeit der Journalisten und schleusen mit gezielten Ködern zur Arbeit Malware auf die Systeme)
        - Grund ist unklar; es wird angenommen, dass z.B. bei einem Ausbruch der Krim Krise vor den Olympischen Spielen in Sotschi, eine kritische Berichterstattung durch staatliche oder staatsnahe russische Organisationen per Cyberangriff unterbunden oder durch Angriffe gezielt geschwächt worden wären
    - Kein echter Schaden ist entstanden
    - Komplexität nimmt zu; Systeme sind vermehrt vernetzt und mobiler und somit nimmt das Gefahrenpotential zu und die Auswirkungen wären dramatischer

3. Wie entgegnen Sie Gefahren im Information Security Bereich?

- **Gibt es ein Risk Management / Wem ist es unterstellt?**

    - Risk Management wird operativ im Rahmen des IT Managements geführt. Unternehmensweit gibt es ein „Corporate Risk Management“, welches strategische und gravierende Risiken dem Verwaltungsrat rapportiert.
    - Aufgrund fehlender Compliance Vorschriften (z.B. SAS70; PCI DSS Kreditkartenverarbeitung; SOX Börsenkotiert U.S.) fehlt der Druck um Risiken einfacher zu definieren und zu bekämpfen
    - Es gibt kein Controlling aufgrund fehlender Compliance Vorschriften
        - Compliance Vorschriften definieren meistens, dass es ein Risikomanagement geben muss; dass es ein Kontrollsystem geben muss etc.
    - Management versteht oft nur Risiken
        - Schwachstellen einer Webseite muss man somit in wenigen Worten (Risiken) dem Management aufzeigen, welche Auswirkung es auf das Unternehmen hat

- **Ist die IT ein essentieller (Risiko-) Faktor der Unternehmung?**

    - Die Infrastruktur (speziell die auch die kritischen ersten Radio Kanäle) werden durch IT Infrastruktur gesteuert (Der Bund könnte daran gehindert werden Informationen zu verbreiten oder Falschinformationen könnten durch Angreifer gezielt für Panik sorgen)
    - IT Risiko als gesamtes definieren und die Aktivitäten an dieses Risiko angliedern (ISO27001 verfolgt einen ähnlichen Ansatz). Es braucht viel Überzeugung des Managements
    - Szenario basierte Erklärungen von möglichen Angriffen sind die besten Arten, es dem Management zu erläutern:
        - Gross-Operationen: was könnte passieren wenn!
        - Normaler Sendebetrieb des Radios: was könnte passieren wenn!
        - Aus diesen Szenarien die Aktivitäten ableiten wie z.B. Identity Access Management, AntiVirus Schutz etc.

- **Was wird unternommen, um diesen Risiken entgegen zu wirken?**
    - Cyber Angriff ist als Risiko definiert (gab es früher in dieser Form nicht)
    - Viel Überzeugungsarbeit um das Management auf die Risiken hinzuweisen und mittels Szenario basierten Fällen die Aktivitäten definieren und umsetzten
        - Dauert aber sehr lange: Ein Risiko zu definieren dauert ungefähr ein Jahr
        - Wenn man es konsequent verfolgt ist es auch nachhaltig, braucht aber seine Zeit
    - Vulnerability Tests von Außen wurden durchgeführt um die Schwachstellen zu identifizieren (Als Reaktion auf Hackerangriffe auf SRG Infrastruktur nach negativer Berichterstattung über China)
- **Gab es Cyber Angriffe jeglicher Art? Schützt man sich speziell?**

  Angriffe siehe oben „vergangenen Angriffe“
- **Wie haben sich die Ausgaben zum Schutz der Informationssicherheit im Anbetracht von Cyber Crime verändert?**

  Aufgrund der realen Angriffe auf die SRG und den identifizierten IT Sicherheitsrisiken ist das Thema “Cyberangriffe” auch auf der Management Agenda. Entsprechende Budgets für strategische Projekte im IT Security Bereich sind so überhaupt erst bereitgestellt worden, um die potentiellen Risiken zu reduzieren. Hiervon sind viele einzelne Projekte betroffen, die sonst nicht finanzierbar gewesen wären.
- **Ist MELANI ein Begriff? In welchem Zusammenhang?**

  MELANI ist ein Begriff, die SRG ist aber nicht Teil des Kernverbunds und erhält somit nicht die frühzeitigen Informationen (Beispiel: OpenSSL Heartbleed Fall vom April 2014, diese Information ging frühzeitig an die Mitglieder des Kernverbundes)

  BAKOM wünscht sich, dass man bei MELANI mehr integriert ist
  SRG gehört zur EBU und ist im Technical Commitee. Dort ist die SRG in der EBU Security Working Group wo man sich im vertraulichem Rahmen austauschen kann

  BAKOM möchte, dass man die erkannten Risiken meldet, was aber auch sehr heikel ist, da man die eigenen Risiken / Unternehmensrisiken nach Außen nicht preisgeben möchte um sich vor Angriffen zu schützen. Es wäre der richtige Weg, aber heikel wenn die Informationen in die falschen Hände geraten.

4. Welche Vorschriften oder Standards müssen/werden von ihrer Unternehmung im Bereich Information Security verfolgt

- **Welche Compliance Anforderungen (SOX, Basel II/III etc.) müssen erfüllt werden und aus welchem Grund?**
    - Keine expliziten Vorgaben
    - Gesetzte und Haftung wie alle anderen Unternehmen
        - Geschäftsleitung haftet persönlich

- Vergleich: Organisationspflicht in Deutschland / Due Care Pflicht USA (http://definitions.uslegal.com/d/due-care/)
- Strafgesetzbuch
- Datenschutz etc.

→ Einfacher wäre es, wenn es ein Gesetz, eine Vorschrift gäbe, welche alle Firmen einer einheitlichen Regelung unterstellt sind, welche im Internet ein Geschäft betreiben. Dies wäre der Weg um wirklich weit zu kommen.

→ Es würde der gesamten Wirtschaft guttun, wenn Firmen welche im Internet zu tun haben, gewisse Vorschriften haben. Es muss nicht viel sein, aber gewisse Punkte müssten definiert werden.

z.B.:
Unternehmen sollten verpflichtet sein ihre IT, vor allem aber die im Internet erreichbaren Systeme angemessen zu betreiben.

Angemessenheit könnte man dann juristisch jeweils als „Best-Practice" (zu diesem Zeitpunkt) auslegen.

Hierunter würde heute fallen:
- Regelmässiges Patching
- Schutz vor Malware
- Schutz personenbezogener Daten
- Einsatz von State of the Art Technologien.

- **Werden Compliance Management Systeme eingesetzt?**

  - An ISO27001 angelehnt (deckt die gesamte Palette gut ab)
    - Besteht aber aus viel Papierarbeit
    - Ziel ist es, ISO27001 kompatibel zu sein; und auf die nächsten Jahre gesehen evtl. auch ISO zertifiziert

- **Gibt es andere Frameworks oder Applikationen welche der Unternehmung helfen, Risiken zu minimieren/verwalten?**

  - Frameworks in diesem Bereich sind oft sehr ähnlich im Gesamten und haben ihre speziellen Eigenheiten. Hat man ISO 27001 dann deckt man einen Grossteil von anderen Frameworks wie z.B. SAS70 ab
  - PCI DSS ist gut, aber etwas genauer definiert was man machen muss
  - Benchmarks vom Center for Internet Security (CIS) in Verbindung mit ISO27001 bilden in etwa dass ab, was der BSI Grundschutz vorgibt
  - BSI Grundschutz ist sehr mühsam zu implementieren (obligatorisch für Deutsche Behörden) ISO27001 zertifiziert auf BSI Grundschutz
    - Modularer Aufbau z.B. Baustein VoIP, Server etc.
    - Endet in einem großen Dokumentationswald
    - Nachteil: nicht sehr pragmatischer Ansatz um Risiken zu minimieren; man hat die Vorgaben erfüllt aber man verliert das Big Picture; das eigentliche Risiko Cyber Angriff wäre somit nicht direkt abgedeckt
    - Die Vorgehensweise ist von Unternehmen von Unternehmen verschieden

- **Gibt es Bereiche welche ihrer Meinung nach zu wenig durch solche Frameworks / Tools unterstützt werden?**

  Viele Frameworks sind sehr abstract. Sie probieren eine Allumfassende Blaupause zu erstellen, was in der Regel aber nicht funktioniert.

  Man kann ein Framework viel einfacher beschreiben, in dem man ein Big-Picture erstellt, was die „relevanten IT Sicherheitsrisiken des Unternehmens“ beschreiben sollte.

  Hier gibt es zu wenige Beispiel. Innerhalb einer Branche sind die Risiken vergleichbar, über Branchen hinweg wird es schwieriger.

  Ein Medien-Risiken-Framework würde hier beispielweise Print und Broadcast helfen, um dann wiederum andere Frameworks angepasst anzuwenden.

- **Was empfinden Sie als Vor- und was als Nachteil von Compliance Vorschriften?**

  Vorteil: Der Druck auf das Management steigt und als Sicherheitsverantwortlicher hat man die Mittel um die Aufmerksamkeit des Managements zu erhalten.
  Nachteil: Formalismus.
  Solche externen Vorgaben bedeuten, dass man auch von externen Prüfern auditiert wird. Dort ist der Kenntnisgrad in der Regel geringer, wodurch man bei jedem Thema quasi von Adam und Eva beginnen muss, erklären muss, wie eine Sendung produziert wird, was dann übergeleitet erklärt, warum man jetzt genau eine Technologie in der aktuellen Form und Konfiguration einsetzt.

  Das endet in Formalismus. Durch die Audits probiert man nicht sicherer zu werden, sondern nur die Audit-Anforderungen zu erfüllen.
  Das führt zu erhöhten und vor allem oft auch fehlgerichteten Aufwänden.

5. Würde ein branchenübergreifendes Information Security Compliance Framework im Bezug auf Cyber Threats mit vorgeschriebenen Audits mehr Sicherheit bringen?

- **Wie stehen Sie einem umfassenden Framework zur Erfüllung von Compliance Anforderungen für kritische Infrastrukturen in der Schweiz gegenüber? Was könnten mögliche Hindernisse sein? Wie wäre die Akzeptanz in den betroffenen Betrieben?**

  Es würde sicherlich einen positiven Einfluss auf die Informationssicherheit haben

  1. Compliance Vorgabe würde helfen: Überzeugung der Geschäftsleitung fällt weg oder wird einfacher
  2. Ein Framework anbieten um die Compliance Vorschriften zu erfüllen
     Dieses Framework sollte aber nicht zwingend sein, sondern soll zu Verfügung stehen wenn man dieses anwenden möchte

  Andere Frameworks sollen auch akzeptiert werden und mittels Audit (durch den Bund) wird die Compliance überprüft. Das Unternehmen muss dann Rechenschaft über die eingesetzten Mittel ablegen, aber die Wahl des Frameworks sollte offengehalten werden

Auf dem Radar der Geschäftsleitung würde dann automatisch Security als relevanter Punkt auftauchen

Z.B. SOX zieht die Geschäftsleitung explizit in die Verantwortung, dass die abgelieferte Arbeiten korrekt ausgeführt wurden. Die Geschäftsleitung ist für das Risikomanagement zuständig etc. und haftet für Non-Compliance.
Dies ist sowieso so, aber es wird dann explizit erwähnt und ist zwingend. Audits sind dann die Driver um entsprechende Maßnahmen korrekt umzusetzen.

Delegierte Personen für diese Aufgabe können dann sofort handeln und müssen nicht mehr Überzeugungsarbeit dem Management gegenüber leisten

Wenn der Bund Vorgaben machen würde, wäre die Abneigung vorerst gross, aber wenn man es über die Jahre durchsetzen würde, dann würde dies sicherlich helfen.
Es gibt einen Grund warum es Gesetze gibt, wenn man nur auf Selbstregulation setzt, kommt es auf die Dauer auch nicht gut.

6. Was ist die grösste Herausforderung in der Informationssicherheit für die nächsten 5 Jahre?

- Technischer Natur: SCADA Systeme / Broadcast Systeme / Industrieanlagen sind immer mehr vernetzt; verwachsen mit der normalen IT
  - Die Fehler welche man früher in der IT machte, tauchen nun in den Produktionssystemen auf
  - Produktionssysteme sind nicht in der gleichen Art und Weise programmiert wie moderne IT Systeme
  - „Never Touch a running System“ gilt in der Industry nach wie vor
  - Web Front Ends sind angreifbar und die Anforderung an die Mobile Steuerung dieser Anlagen ist ein Problem
- Endbenutzer: Fahrlässigkeit der Endbenutzer ist ein Problem. Der Mensch wird zur grössten Schwachstelle, zum schwächsten Glied. Es reicht nicht aus die Technik sicher zu machen. Passwörter müssen komplex sein und häufig gewechselt werden, dies muss der Mensch machen.

  Früher hat man sich auch nicht im Auto angeschnallt und heute machen es praktisch alle. Es ist ein Prozess den der Mensch durchgehen muss. Das Verständnis für die Auswirkungen muss geschaffen werden.

  → Bewusstsein für die Konsequenzen

  → Persönliches Risiko Management

  - Weiter ist es schwierig, die Security als Mehrwert und nicht als Verhinderer wahrzunehmen. Man schafft eine Sicherheit, man schafft einen Mehrwert für den Menschen und die Unternehmung

10.1.4 Mark Lütz, Swisscom

- Name: Mark Lütz
- Firma: Swisscom
- Position: Infrastructure Customer Unit - CISO Outsourcing

1. Was macht ihre Unternehmung zu einem Teil der kritischen Infrastrukturen?

- **Zählen Sie die Unternehmung als Teil der kritischen Infrastrukturen der Schweiz?**

  Ja dies ist definitiv der Fall, der Bund definiert die kritischen Infrastrukturen. Abhängigkeiten bestehen zu Unternehmen wie der SBB, Energiebehörden, Blaulicht Organisationen welche sich oft auf eine Infrastruktur der Swisscom verlassen. Sei dies das Backbone Netzwerk oder Mobile Infrastruktur

  Grundschutzabdeckung als Auftrag
  Swisscom BCM/DR Strategie für die nationalen Standorte ist definiert und wird je nach Ausprägung über das Crisis Mgmt. im Ernstfall gesteuert. Weniger ist dabei mehr für kurze zielführende Mitigationen. Die Frage muss man sich stellen: Was passiert wenn die Swisscom Infrastruktur heruntergefahren werden muss

- **Was sind die wichtigsten Assets der Unternehmung?**

  - Backbone (viele schweizerische Unternehmen sind auf das Backbone der Swisscom angewiesen) und die Schweizer Netzinfrastruktur.
  - Abhängigkeit zu globalem Netz (Mashing)
  - Operation der Datacenter (im BCM & DR Fall sind die verfügbare Personen wichtig)
  - Logisches Asset ist auch das DDOS Protection System der Swisscom (DDOS Battles welche zu einem nationalen kollateral Schaden führen können)

- **Was wird als grösster Risikofaktor angeschaut? Was wäre ein GAU?**

  - Pandemie
  - Supervulkan (Asche) und Erdbeben
  - DDOS Attacken
  - Abhängigkeit unter den Providern

2. Welche Angriffe auf (Information) Assets der Unternehmung gab es in den letzten 10 Jahren?

- **Gab es in den letzten 10 Jahren einen grösseren Zwischenfall in Bezug auf Informationssicherheitsverletzung?**

  - Postfinance Fall (DDOS Attacke)
  - Überschwemmung beim Titlis (Infrastruktur der Swisscom)
  - IPSS (MPLS CH) Failover hat nicht korrekt funktioniert → Westschweiz ohne Netzwerk / Fehlendes realitätsnahes Testing zum Teil nicht mögilch

  Unerlaubte Zugriffe (aus Schweizer Sicht) von extorialen Intelligence Services auf Daten

→ Wie kann es sein, dass man als Schweizer Firma die Daten in einer Cloud speichert, wobei man den Standort der Daten nicht kennt (Wo liegen meine Daten? Silicon Valley?)

Wichtig sind:
- Zonenkonzept
- Vulnerability Management
- Data Leakage Prevention (Vertrauen ist gut, Kontrolle ist besser; wo gibt es Tendenzen?)
- Prozesse und Organisation
  - Swisscom Tap Issue (Taps sind verschwunden, wie konnte dies passieren? Wurden Kundendaten entwendet?
  - Nach ISO27001: Control & Verification: Kontrolle wer hat den Fehler gemacht
  - Wenn es Issues gibt, muss dies Nachvollziehbar sein
  - Verbesserungen durch verbesserte Kontrollen im RZ etc. aber dieses System ist nur so gut wie die Hintertüren ebenfalls gesichert sind.
  - In der Cloud ist es nicht anders
  - Wie sieht die ISO27002
- Standort Schweiz als Cloud Data Standort kann wichtig sein
  - Aufbau sollte durch Swisscom selbst stattfinden ohne ausländische Partner
  - Engineering sollte nicht ausgelagert werden
  - Kunden möchten nicht, dass ihre Daten im Ausland lagern

3. Wie entgegnen Sie Gefahren im Information Security Bereich?

- **Gibt es ein Risk Management / Wem ist es unterstellt?**

Ja es gibt ein Risk Management nach ISO27001. Übergeordnet in den Konzernbereichen für Residential (Enduser) oder Enterprise Business im allg. und Security Risk Mgmt.
Z.B. FINMA setzt ein Risk Management für Kunden der Swisscom voraus welche somit auch von der Swisscom in diesem Bereich erfüllt werden muss
Unterscheiden zwischen:
- reputation damage risk
- commercial risk
- operational risk

Nicht nur vom Risk Management sprechen, aber von Risk Mitigation.
Finma Rundschreiben 2008-21, Im speziellen Anhang 3: Umgang mit elektronischen Kundendaten.
Neue/angepasste Grundsätze mit entspr. Impakt Szenarien:
- Governance
- Kundenidentifikationsdaten
- Datenspeicherort und –zugriff
- Sicherheitsstandards für die Infrastruktur und die Technologie
- Auswahl, Überwachung und Schulung von Mitarbeitenden, die auf CID Zugriff haben
- Risikoidentifizierung und -kontrolle in Bezug auf die CID-Vertraulichkeit
- Risikominderung in Bezug auf die CID-Vertraulichkeit

  - Vorfälle im Zusammenhang mit der CID-Vertraulichkeit, interne und externe Kommunikation
  - Outsourcing-Dienstleistungen und Grossaufträge in Verbindung mit CID

Wichtig ist, dass zwischen GRC unterschieden wird. Langfristige Reputation Risks sind sehr relevant

- **Ist die IT ein essentieller (Risiko-) Faktor der Unternehmung?**

  IT ist ein essentieller Faktor der Swisscom. Ein Totalausfall auf die IT Infrastruktur würde den Betrieb stark beeinflussen

- **Was wird unternommen, um diesen Risiken entgegen zu wirken?**

  - Zonenkonzept der IT Infrastruktur
  - Vulnerability Tests
  - Data Leakage Prevenation
  - Swisscom Public/Private Cloud Hosting in der Schweiz
  - Realitätsnahe Failovertests (Im Live Environment ist dies nicht zu verantworten und deshalb kann man es nur möglichst realitätsnah aber nie 1 zu 1 testen)

- **Gab es Cyber Angriffe jeglicher Art? Schützt man sich speziell?**

  DDOS Attacke auf Kunden welche über die Swisscom angebunden sind und vom DDOS Protection Service der Swisscom geschützt werden

- **Wie haben sich die Ausgaben zum Schutz der Informationssicherheit im Anbetracht von Cyber Crime verändert?**

  Neue Business Cases wie Machine2Machine (Hinweis Zusammenarbeit mit Schindler Lifte)
  Wie werden diese Anlagen gesichert? Wie könnte ein Angriff auf diese Systeme aussehen? Wie sieht die Umsetzung aus um diese Angriff Szenarien zu schützen. Da müsste noch mehr investiert werden. Solange nichts passiert wird wenig gemacht. Group Control müsste hier greifen und auf diesen Risiken aufsetzen.

- **Ist MELANI ein Begriff? In welchem Zusammenhang?**

  Ja ist es, aber intern gibt es keine Vorgaben bzw. Anstösse diese Plattform zu nutzen.

4. Welche Vorschriften oder Standards müssen/werden von ihrer Unternehmung im Bereich Information Security verfolgt

- Welche Compliance Anforderungen (SOX, Basel II/III etc.,) müssen erfüllt werden und aus welchem Grund?
  - Grundsätzlich wird auf ISO 27001/ (27002 für die Control Validierung) aufgebaut
  - In welchem Bereich muss die Swisscom zu welchen Regulations compliant sein
  - Z.B. Trading Platform
  - Ansatz wäre, über alle Shared Services FINMA compliant zu sein

- Somit könnte man der FINMA für Kunde X die geforderten KPIs ausliefern
- Periodischer Review ist sehr wichtig
  - Änderungen wie das Attachment 3 des FINMA muss entsprechend overall umgesetzt werden
  - Dedicated Services sind dabei sehr aufwendig (Kunde fordert Änderungen per Change an und dann wird dies umgesetzt)
  - Auditors der FINMA kommen in Zukunft direkt auf die Provider zu und werden nicht mehr durch die Kunden gestellt (zb. Internen Konzern Auditors von Kunden)
  - Audits werden dadurch viel aufwendiger

Firmen kommen mit Anforderungen: ihr müsst nach bestimmten Regulationen für die Schweiz compliant sein
Beispiel: Lync monitoring – IP Adressen der Schweiz dürfen die Schweiz nicht verlassen
Jedes Land hat eigene Auflagen / erfordert getrennte Architekturen etc.

Wichtig: Technologie und Legal Compliance und Gesamtcompliance muss man zusammenfassen

Keine SOX Relevanz: SOX Control ist intern kein Thema. Beim Kunden kann dies ein Thema sein. Nur in den Bereichen wo der Kunde dies erfordert werden diese umgesetzt
Basel II/III

- **Werden Compliance Management Systeme eingesetzt?**

  Unterscheiden zwischen G R und C
  Swisscom Enterprise (neue Legal Entity nach Gründung) hat ein Application Lifecycle Mgmt. (ALM) mit dem man die Sec&compliance controls über Platformen und auch die 27002 controls prüfen kann.

- **Gibt es andere Instrumente und Standards (Frameworks, Applications etc.) welche der Unternehmung helfen, Risiken zu minimieren/verwalten?**

  Compliance control frameworks:
  Lebendiger prozess. Anwendbarkeit ist nur so gut, wie die nachhaltige Evidence Review funktioniert.

  Kunden verwenden nicht Standard Produkte / Systeme. Nach ISO27000 verwenden wir Standart Systeme. Somit müsste man sich auf diese Systeme anpassen damit die Controls korrekt durchgeführt werden können.

  Swisscom ist auf gutem Wege; Systeme können eingeführt werden; Management denkt, man kann es nur bei Standard Services anwenden. Dedicated Services für Banken fallen dann ab. Es fehlen dann die Kontrollverifikationen. Deswegen ist es schwierig, ein übergreifendes Control Framework in der Swisscom einzuführen

Der Einsatz von Tufin/Algosec/Skybox kann sehr hilfreich sein um das Change und Policy Management zu verbessern. Es hilft für eine saubere Implementierung und das House Keeping.
Diese Tools werden noch zu wenig eingesetzt. Vor allen Dingen im Hinblick auf integrierte Workflows.

- **Gibt es Bereiche welche ihrer Meinung nach zu wenig durch solche Frameworks / Tools unterstützt werden?**

  SLA und SLA LVL Mgmt. für SLA Breach und Treshold Impact und den damit verbundenen Controls. Breakfixing (Fieldforce) und über neue Standardservices in einem Partnershipment wo es gilt sauber orchestieren zu können.

- **Was empfinden Sie als Vor- und was als Nachteil von Compliance Vorschriften?**

  Problem ist zwischen Business und IT
  Business Risk müssen definiert werden. Interessant ist, dass die Kritikalität sinkt, sobald man aufbauen auf diesen Risiken die IT Risiken definiert werden und dafür das Budget gesprochen werden müsste

5. Würde ein branchenübergreifendes Information Security Compliance Framework mit vorgeschriebenen Audits mehr Sicherheit bringen?

- **Wie stehen Sie einem umfassenden Framework zur Erfüllung von Compliance Anforderungen für kritische Infrastrukturen in der Schweiz gegenüber? Was könnten mögliche Hindernisse sein? Wie wäre die Akzeptanz in den betroffenen Betrieben?**

  Grundlegende Mechanismen von Cobit / ITIL können Enabler sein
  Können für Systemübgreifende Systeme hilfreich sein.
  Zusammenarbeit zwischen Providern und Abhängigkeiten könnten vereinheitlicht werden
  Generische Anforderungen definieren: für Vulnerability und BCM z.b.

  Framework kann helfen, für unerfahrenere Bereiche welche sich im Wandel auf digitale Systeme durchlaufen, einen Grundschutz aufstellen und gewisse Bereiche abdecken (wie BCM, Vulnerability Management, Zoning, etc.)

  Könnte einen guten Effort geben und übergreifend ein Improvement geben. Löst aber keine spezifischen Zusatzlösungen ab, welche für die einzelnen Bereiche speziell vorhanden sein müssen / sind

  Hindernisse: Faktor Mensch; bin ich in der Lage die Risiken kritisch zu überprüfen; Weiterbildung, technische und prozessorientierte Weiterentwicklung. Nichts ist so schnell wie der Wandel. Nicht nur theoretische sondern auch praktische Erfahrung muss vorhanden sein.
  Manchmal ist weniger mehr. Das wenige richtig machen! Die letzten 10% sind oft sehr teuer diese umzusetzen.

6. Was ist die grösste Herausforderung in der Informationssicherheit für die nächsten 5 Jahre?

Grösste Herausforderung ist es, einen grossen Kollateralschaden abzuwenden bzw. Risiken zu minimieren. Dies kann erreicht werden durch z.B.:

- Perimeter Sicherheit (wir können und wollen mit allen kommunizieren aber mit Einschränkungen)
- Zonenkonzept: DMZ mit abwägen der Risiken und deren Eintrittswahrscheinlichkeit. Man nimmt gewisse Risiken in Kauf oder steckt heikle Daten in eine High Secure Server Zone
- Vertrauen in Hersteller ist sehr gross, die Erfahrung zeigt aber, dass z.b. Würmer in Hersteller Software stecken welche man nicht erwartet hätte.

Wandel:

- früher gezielte kriminelle Angriff mit dem Ziel Geld zu ergaunern
- Globale Angriffe (z.b. DDOS) auf globale Techniken sind erfolgreich (Stichwort OpenSSL Heartbleed); wer steckt dahinter und wer nutzt dies aus?
- Politisch und Business motivierte Angriffe sind viel stärker und haben zugenommen

Gefahren lauern bei:

- interne Ausspähung
- mobile Abhörung

Die Fragen die sich dabei stellen:

- müssen wir dies alles haben? Z.B. BYOD soll in einer Sandbox laufen

Weitere Punkte sind:

- Digitalisierung z.B. SCADA Systeme von Kernkraftwerk (Steuerung von wichtigen Komponenten wie Kühlbecken, Spannungsregler). Wie schützt man diese Komponenten angemessen etc.
- Datenschutzrechtliche Aspekte (privater Datenschutz, Schutz von Mitarbeiterdaten)
- Korrelation der Daten ist enorm wichtig aber auch kritisch: Stichwort NSA / Wirtschaftsspionage

10.1.5 Andy Mühlheim, Swissgrid

- Name: Andy Mühlheim
- Firma: Swissgrid
- Position: CIO

1. Was macht ihre Unternehmung zu einem Teil der kritischen Infrastrukturen?

- **Zählen Sie die Unternehmung als Teil der kritischen Infrastrukturen der Schweiz?**
    - Swissgrid zählt zu den superkritischen Infrastrukturen der Schweiz, gleiche Stufe wie die Telekommunikationsinfrastruktur
    - Die Abhängigkeiten anderer Infrastrukturen vom Stromnetzwerk ist sehr groß
- **Was sind die wichtigsten Assets der Unternehmung?**

  Die Umgebungen der swissgrid werden in drei Bereiche eingeteilt und mit einer Kritikalität versehen
    - Bürozone
    - Umsysteme und unterstützende System
    - Steuer und Leitsysteme / Produktionszone

  Gesamte IT Systemlandschaft kann als wichtiges Asset angeschaut werden
- **Was wird als grösster Risikofaktor angeschaut? Was wäre ein GAU?**

  Grösster Ausfall wäre ein Zusammenbruch des Elektrizitätsübertragungsnetzwerkes. Die Übertragung könnte nicht mehr sichergestellt werden und grosse Teile der Schweiz (und u.U. auch im angrenzenden Ausland) wären ohne Strom. Grosse Abhängigkeiten der Bevölkerung und anderer Unternehmen
  Als Risiko wird auch Cyber Risk und die Vernetzung von industriellen IT Systemen angesehen.

2. Welche Angriffe auf (Information) Assets der Unternehmung gab es in den letzten 10 Jahren?

Swissgrid geht generell davon aus dass man ein Ziel von Angriffen ist
Man verzeichnet auf den Perimeter Firewalls eine grosse Anzahl unautorisierte Anfragen.
Ausfälle der Infrastruktur gab es in der Vergangenheit ebenfalls, welche aber nicht direkt auf Angriffe als eher Unfälle zurückzuführen sind. Redundanzen verhinderten dabei einen Totalsausfall.

3. Wie entgegnen Sie Gefahren im Information Security Bereich?

- **Wie sieht das Riskmanagement aus?**
    - Risiko: man ist grundsätzlich angreifbar und wird angegriffen
    - Risiko Management von abhängigen Unternehmen ist aus der Sicht von swissgrid oft zu schwach. Man ist für einen großflächigen Stromausfall kaum gewappnet. End-to-End View muss im Risiko Management berücksichtigt

werden. Energieversorgung sollte theoretisch in jedem Risk Management ein Thema sein, man müsste sich de Risiken der Abhängigkeit bewusst sein.
    - Anforderungen von kritischen Infrastrukturen an IT Infrastrukturen können durch die Provider oft nicht erfüllt werden bzw. weitere Investitionen sind notwendig um die BCM Verfügbarkeit zu gewährleisten.

- **Ist die IT ein essentieller (Risiko-) Faktor der Unternehmung?**

  Der Energiefluss bzw. die Schaltanlagen werden durch IT gesteuert.
  Man unterscheidet in der swissgrid nicht zwischen IT und Steuerungsnetzwerken, da alle (mit Ausnahme von wenigen alten Systemen) mittels IT gesteuert werden.

- **Was wird unternommen, um diesen Risiken entgegen zu wirken? Gab es Cyber Angriffe jeglicher Art? Schützt man sich speziell?**

    - Proaktiv Risiken erkennen durch vorgelagerte Sensoren (nicht nur im eigenen Netzwerk)
    - Austausch von Informationen mit Verbundspartner innerhalb Europa
    - Aktive Zusammenarbeit mit Projekten des Bundes im Bereich „Schutz kritischer Infrastrukturen“ Leitfaden und Cyber Defense Strategie
    - Ziel ist es, die Angriffe möglichst zu erkennen bzw. sich dagegen zu schützen bevor diese auf den Perimeter der swissgrid aufprallen

- **Wie haben sich die Ausgaben zum Schutz der Informationssicherheit im Anbetracht von Cyber Crime verändert?**

    - Ausbildung von IT Sicherheitsexperten ist schwierig da das Angebot klein ist
    - Mehrere Mitarbeiter bilden sich in diesem Bereich weiter
    - Pilotprojekt für die Umsetzung des SKI Leitfadens findet statt
    - Eine Grauzone besteht darin, dass Praxisübungen kaum machbar sind

- **Ist MELANI ein Begriff? In welchem Zusammenhang?**

    - Swissgrid nimmt am Austausch von Informationen teil
    - in allgemeinen Bereichen liefert MELANI nützliche Informationen
    - im branchenspezifischen Umfeld fließen die Informationen zusätzlich unter den Branchenpartnern

4. Welche Vorschriften oder Standards müssen/werden von ihrer Unternehmung im Bereich Information Security verfolgt

- **Welche Compliance Anforderungen (SOX, Basel II/III etc.) müssen erfüllt werden und aus welchem Grund?**

    - Es gibt keine bindenden Vorgaben für kritische Infrastrukturen (wie z.B. NERC)
    - Swissgrid wirkte bei der Erarbeitung des SKI Leitfaden und Cyber Defense Strategy des BABS mit
    - NERC Standards werden angewandt wo sie sinnvoll sind

  - Cyber Defense Strategy hat noch Bedarf zur Weiterentwicklung; Jeder Anwender ist selbst verantwortlich / keine zwingenden Anforderungen durch den Bund

- **Gibt es Bereiche welche ihrer Meinung nach zu wenig durch solche Frameworks / Tools unterstützt werden?**

  Für kritische Infrastrukturen in der Schweiz gibt es keinen Standard welcher zur Zeit zur Verfügung steht

- **Was empfinden Sie als Vor- und was als Nachteil von Compliance Vorschriften?**

  Vorgaben erfordern oft nur minimale Sicherheitsstandards und müssen individuell erweitert und angewandt werden
  Risiken im Bereich von kritischen Infrastrukturen tragen nicht die Provider alleine sondern vor allem alle abhängigen Unternehmen und Personen
  z.B. Swissgrid kann nicht die Risiken für alle Unternehmen tragen, welche Abhängigkeiten zum Stromnetzwerk haben.

5. Würde ein branchenübergreifendes Information Security Compliance Framework mit vorgeschriebenen Audits mehr Sicherheit bringen?

- **Wie stehen Sie einem umfassenden Framework zur Erfüllung von Compliance Anforderungen für kritische Infrastrukturen in der Schweiz gegenüber? Was könnten mögliche Hindernisse sein? Wie wäre die Akzeptanz in den betroffenen Betrieben?**

  Es bestehen Unterschiede der Kritikalität (Bund muss Kritikalität vorgeben)
  Swissgrid (Übertragungsnetzwerkbetreiber) hat z.B. eine grössere Kritikalität als ein einzelnes Kraftwerk da das Netzwerk so ausgelegt ist, dass ein Ausfall (auch eines AKWs) leitungsmäßig im Notfall aufgefangen werden kann.
  Hingegen ist der Energiefluss auf der Nord-Süd-Achse sehr wichtig und kritisch.
  Der Staat müsste Vorgaben machen und definieren wie gross ist der Risikoappetit (Risiko wird von allen abhängigen Stakeholdern getragen!):
    - welches Risiko möchte man nehmen / welche Risiken kann man minimieren
    - was ist man bereit dafür auszugeben

  → Mindeststandard an kritischen Infrastrukturen / Anlehnung an NERC Standard denkbar?
  Risiken müssen im Gesamtkontext und nicht nur im Cyber Aspekt angeschaut und korreliert werden. Schutz gegen Cyberangriffe schützt nicht vor Angriffe auf die physischen Infrastrukturen etc.
  BCM spielt dabei eine wichtige Rolle. Wie reagiert man auf einen Unfall und wie stellt man den Services wieder her. Komplette Elimination von allen Risiken ist nicht möglich – man muss davon ausgehen dass man getroffen wird.
  Welche Investitionen möchte man in BCM tätigen? Alternative Pläne / Szenarien / Investitionen in Parallelsysteme / zusätzliche Kapazitäten; firmenübergreifendes BCM muss für kritische Infrastrukturen eingeführt werden. End-to-End View beachten.

6. Was ist die grösste Herausforderung in der Informationssicherheit für die nächsten 5 Jahre?

Die Gesellschaft muss erkennen und verstehen, dass Basisinfrastrukturen wie Energie- und Wasserversorgung, Internet etc. nicht selbstverständlich sind und diese Dienste entsprechende Kosten für den sicheren und zuverlässigen Betrieb mit sich bringen.
Die Bevölkerung ist zur Zeit nicht bereit für den Ausbau des Energieübertragungsnetzwerkes zusätzliches Mittel bereitstellen. Das Verständnis für die Notwendigkeit ist nicht vorhanden: Kosten dürfen keine entstehen aber der Service muss immer in geforderter Qualität zur Verfügung stehen – was auf die Dauer nicht gutgehen kann.
Anderes Beispiel: Funkantennen möchte niemand auf dem eigenen Hausdach, aber der Empfang muss immer in bester Qualität zur Verfügung stehen

- Bewusstsein in der Bevölkerung schaffen / Basis Infrastrukturen ist nicht gratis
- Verständnis für den Risikoträger schaffen / wer ist der Risikoträger (Gesellschaft)
- Abwehr fängt vor und nicht erst auf der Perimeter Firewall an / End-to-End View: Alle Vektoren und Stufen mit einbeziehen

10.1.6Anna Aquilina, Ernst & Young

- Name: Anna Aquilina
- Firma: Ernst & Young
- Position: Director of the EMEIA Information Security Centre of Excellence

What are typical and often used Instruments and Standards for Information Security?

- I believe ISO 27001 will remain the basic standard for Info Sec along with CSA for cloud but others are emerging

How can mandatory standards or common framework support CI's?

- I do not believe Standards are the answer either, but similarly provide a crucial baseline from which organisations and governments can improve/tailor
- Reporting of and penalties for breaches (and transparency of this) are likely to have more of an effect on behaviour than mandatory regulation
- However NIST or another model could be promoted as a global model

What will be the biggest challenges in the future?

- SCADA and embedded technology becoming 'connected' - new for many areas in critical infrastructure
- Mobility and increased remote access
- Employee behaviour
- Need a well-rehearsed CERT environment, clear lines of communication and control. This needs to be adapted to the cyber environment from how it has been traditionally for critical infrastructure

10.2 List of critical infrastructure sectors and subsectors in Switzerland

Sectors	Subsectors
Public administration	Parliament, government, justice, administration
	Research institutes
	National cultural property
	Foreign representations and headquarters of international organisations
Chemical industry	Production, transport, storage, and processing of chemicals
Energy	Power supply
	Oil supply
	Natural gas supply
Waste disposal	Wastewater
	Industrial and domestic waste
	Special waste
Financial services	Banks
	Insurance companies
Public health	Medical care and hospitals
	Medicine
	Laboratories
Information and communication technology (ICT)	Telecommunications
	Information systems and networks
	Internet
	Instrumentation, automation and monitoring systems
	Radio and media
Water and Food	Food supply and food security
	Potable water supply
Public safety, rescue, and emergency services	Emergency organisations (police, fire service, emergency health care and rescue services)
	Civil protection
	Armed forces
Transport	Road transport
	Rail transport
	Air transport
	Navigation
	Postal services and logistics

	Very high criticality*
	High criticality*
	Regular criticality*

*
► All subsectors are critical.
► Criticality refers to the importance of the subsector in terms of interdependency, the population, and the economy (not its general importance or its mission-criticality).
► Even subsectors whose criticality is regular may contain highly critical individual elements.
► Weighting is based on an ordinary threat level. *

Figure 11: Critical infrastructure sectors and subsectors in Switzerland (Source: FOCP 2009b)

10.3 CIISM Maturity Model Approach

A maturity model should provide a benchmark for CIE to evaluate their information security level and capability to improve their resilience against damage through information loss and manipulation.

The component maturity model gives the responsible authority the ability to measure the level of all relevant CIE's and set goals for improvement to gain an increased overall level in each CI section. (DHS 2014)

Different levels can be appropriate for different parts of an enterprise network. Table 25 lists a proposal of maturity levels (ML) for apply information security measures defined by CIISM.

Table 25: Proposal of CIISM maturity levels

ML0	No mandatory information security minimum standards are applied
ML1	Minimum standards are applied; recommended for administrative section which are part of the CIE but can be completely run isolated of critical parts
ML2	Medium maturity level implemented; recommended for an environment which is used for running critical parts but is not directly or permanent connected to them
ML3	Highest security implementation applied; strongly recommended for all systems and operators that have direct access to critical parts like ICS