Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Finance FDF
Federal IT Steering Unit FITSU

National Strategy for the Protection of Switzerland against Cyber Risks

NCS implementation plan

15 May 2013

Contents

1 Background

On 27 June 2012, the Federal Council ratified the national strategy for the protection of Switzerland against cyber risks (the NCS), laying the foundations for a comprehensive approach to tackling cyber crime. The NCS seeks to improve the early detection of cyber risks and emerging threats, make Swiss infrastructure as a whole more resilient to cyber attacks and generally reduce cyber risks. The strategy comprises 16 individual action points (measures), broken down into seven spheres of action. The aspiration is that these will be in place and in regular use by 2017.

The spheres of action and individual action points (measures) are as follows:

Sphere of action 1	**Measures**	
Research and Development	1	New cyber risks connected with related problems must be researched
Sphere of action 2	**Measures**	
Risk and vulnerability analysis	2	Independent evaluation of systems Risk analyses to minimise risks in collaboration with authorities, ICT-service or system providers
	3	Examine ICT infrastructure for systematic, organisational or technical vulnerabilities
Sphere of action 3	**Measures**	
Analysis of the threat landscape	4	Establish a picture of the situationand its development
	5	Review of incidents for the development of measures
	6	Overview of cases and coordination of inter-cantonal complex cases
Sphere of action 4	**Measures**	
Competence building	7	Establish an overview of competence building offers and identification of deficiencies
	8	Filling in of gaps in competence building and increased use of high quality offers
Sphere of action 5	**Measures**	
International relations and initiatives	9	Active participation of Switzerland in Internet governance
	10	Cooperation at the international security policy level
	11	Coordination of actors involved in initiatives and best practices, relating to security or assurance processes
Sphere of action 6	**Measures**	
Continuity and crisis management	12	Strengthening and improvement of resilience towards disturbances and incidents
	13	Coordination of activities, primarily with directly involved actors and support of decision-making processes with expertise
	14	Active measures to identify the perpetrator and possible impairment of its infrastructure in the event of a specific threat
	15	Elaboration of a concept for management procedures and processes to resolve problems in good time
Sphere of action 7	**Measures**	
Legal basis	16	Evaluation of existing legislation on the basis of measures and implementation concepts and priorisation of immediate adjustment needs.

Underpinning the strategy is the assumption that cyber risks are a manifestation of existing risks in processes and structures. Cyber risks arise from the use of (interconnected) ICT systems, which are now increasingly called upon to perform and operate all sorts of processes, from sending e-mails instead of letters to the computerisation of highly complex control and production systems instead of its manual operation. Identifying cyber risks thus entails having to assess the actual threat situation for individual ICT-based processes and their interconnectedness as precisely as possible. However, implementation of security measures to minimise cyber risks should not be limited to the sphere of ICT security only: such measures

must always address and relate to the physical, human, technical and organisational dimensions. At a national level, this is possible only through interconnecting the different measures with each individual taking personal responsibility.

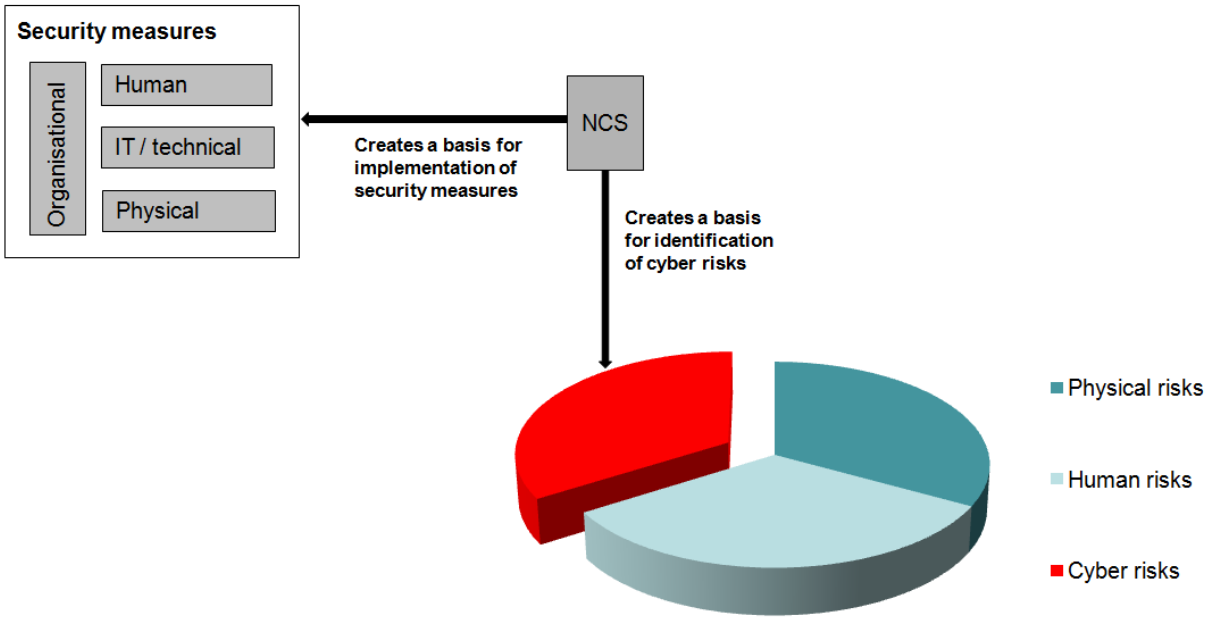

Figure 1: Cyber risks and security measures

Implementation of the strategy will be coordinated by a coordination unit within the FDF, or more specifically, the Federal IT Steering Unit (FITSU). Together with the corresponding bodies at the federal level and their partners in the cantons, this coordination unit will draw up an implementation plan for the strategy and clarify in detail any additional human resources that may be required in the participating federal government departments and the Federal Chancellery from 2014 onwards.

Regarding the protection of Switzerland's critical infrastructure (CI), the NCS strategy builds upon the national strategy for the protection of critical infrastructures (SKI strategy) from the Federal Office for Civil Protection (FOCP). As the risk and vulnerability analyses envisaged under the SKI programme are also supposed to identify cyber risks, this should form the basis for harmonised, sector-specific risk minimisation. The risk and vulnerability analyses take account of the sectors and sub-sectors defined in the SKI strategy. This process involves the relevant regulators and supervisory bodies in each case as well as the Federal Office for National Economic Supply (FONES) and the Federal Office for Civil Protection (FOCP). The FONES[1] and the FOCP[2] are charged with compiling a risk and vulnerability analysis for their respective sub-sectors. Wherever possible and relevant, these two federal offices should agree upon the procedure and methods to be used, adopting an approach that is as consistent as possible.

[1] The 13 sub-sectors of the FONES are: energy (natural gas supply; mineral oil supply; electricity supply), industry (chemicals and medicines; mechanical and electrical engineering industries), information and communication technologies (information technologies; telecommunication), provisions (food supplies; water supply), transport and logistics (air transport; rail transport; sea transport; road transport).

[2] The 15 sub-sectors of the FOCP are: public authorities (Parliament, the judicial system and administration; research and teaching; cultural artefacts; international organisations), waste (waste water; waste disposal), finance (banks; insurance companies), health (medical care and hospitals; laboratories), information and communication (media; postal service), public security (armed forces; emergency services; civil protection).

The results are consolidated in collaboration with the Reporting and Analysis Centre for Information Assurance (MELANI) to form a comprehensive analysis of the threat situation.

The areas of overlap and dependence with respect to the SKI strategy can be summarised as follows:

- The national SKI strategy serves as an overarching strategy for protecting Switzerland's critical infrastructures. The NCS strategy covers the protection of critical infrastructures from cyber threats.
- Measures under the NCS strategy that concern critical infrastructures are aligned with the corresponding measures in the SKI strategy (e.g. risk and vulnerability analyses).
- Implementation of NCS measures concerning critical infrastructures is closely coordinated between the FONES, the FOCP and the FITSU.

To define the details of the measures, the NCS coordination unit interviewed representatives of the federal offices involved (see Chapter 7) and then compiled and consolidated its findings. This entailed analysing the current state of progress and further planning for the implementation of the strategy were considered. The key findings were as follows:

a) The approach of corporate (self-) responsibility with the Confederation playing a subsidiary role, as set out in the strategy, is correct.
b) Following completion of the planned risk and vulnerability analyses, further action and additional costs, which might arise on the basis of overriding national interests, may become necessary in order to eliminate existing risks.
c) Some federal departments have already taken preliminary steps to implement the measures within the framework of their remit.
d) The resource requirements must be clearly demonstrated.

This implementation plan from the FDF forms the basis for the federal departments and offices to clarify and implement the appropriate measures. However, it does not specify the tasks and duties of the new positions to be set up; this is clearly left to the individual organisations to ascertain, based on its experience in day-to-day operations. The point of departure is the set of measures outlined in the strategy, which are to be put in place and made part of day to day operations by end 2017.

The cantons will be included in this implementation process through the consultation and coordination mechanism of the Swiss Security Network (KKM SVS). Furthermore, in association with the KKM SVS, the NCS coordination unit will support a cyber expert group consisting of federal, cantonal and municipal representatives.

The NCS explicitly excludes the case of war and conflict. The armed forces are responsible for protecting and defending their own infrastructure and systems in all situations. They should also define approaches to tackle cyber threats and their consequences within their own area of action and responsibility. To this end, the Chief of Staff has appointed an Armed Forces Cyber Defence Delegate, who assumed his position on 1 January 2013.

2 Remit and Framework Conditions

As the plans for strengthening security in the cyber domain can only be achieved through interaction between the federal administration, cantonal authorities, economic sectors/subsectors and critical infrastructure (CI) operators, the strategy incorporates all of these stakeholders in the implementation process.

The implementation plan was prepared with the close involvement of the Federal Office for National Economic Supply (FONES) and the Federal Office for Civil Protection (FOCP). The consultation and coordination mechanism of the Swiss Security Network (KKM SVS), which forms the point of interface between the Confederation and the cantons, was also a key implementation partner.

3 Findings

3.1 Resource Requirements

The estimated requirements, which were consolidated in the interviews, are based on existing estimates of requirements and position papers from the relevant offices in this area or have been derived from the measures set out in this strategy. Given the additional workload involved in identifying the cyber aspects associated with existing processes in the federal administration, for implementation of the NCS measures, there is a need for additional resources.

Expertise on similar cyber aspects is required in numerous federal offices. Suitable forms of cooperation have been discussed to build up and share this knowledge together, e.g. in the regulatory area, where synergies arise for authorities such as the Federal Office of Civil Aviation (FOCA), the Federal Roads Office (FEDRO), and the Swiss Federal Office of Energy (SFOE). Here, there is a need for joint discussion on, for example, amplification of cyber risks through increased use of management and control systems. The same individuals could also participate occasionally in inspections concerning cyber-specific areas. It has yet to be clarified whether and to what extent the federal departments could meet this need with an expert pool of subject-specific specialists, whose expertise could then be made available to the individual offices.

The NCS strategy has extended the basic remit of MELANI (DDPS and FDF), which is now required as part of this implementation plan to provide additional services. These include analysis on current status, support and follow-up of incidents, and support for risk and vulnerability analyses by CI operators. Furthermore, ICT service providers and system suppliers will be more closely involved in MELANI. MELANI thus fulfils a key role in implementing the measures of the strategy by taking charge of the coordination, evaluation and forwarding of information concerning the tackling of cyber risks and by ensuring an exchange of information with the CI operators, the relevant ICT service providers and system suppliers. The resulting information hub to be created lies at the heart of the strategy. Upon completion of the implementation process at the end of 2017, MELANI will, where necessary, assume a coordination and management function within its remit. The tasks of MELANI are therefore listed separately in the following table.

Federal department	New posts	Staff reduction by end-2017	NCS measures to be implemented
FDFA	+2	0	7;8;9;10;11;13
FDJP	+1	-1	4;6;13;14
DDPS	+17	0	2;3;4;5;6;11;12;13;14
FDF	+6	-1	2;3;4;5;6;7;8;9;10;11;12;13;14;16
EAER	+2	0	2;12;13
DETEC	+2	0	2;3;7;8;9;10;11;12
Total	+30	-2	
MELANI (resources already listed under FDF + DDPS)	+6	0	2;3;4;5;6;10;11;12;13;14

3.2 Relevance of Sectors, Sub-sectors and CI Operators

The Confederation can have only limited success in building national cyber resilience through its own measures. The declared federal expenses serve to create the optimum framework conditions for improving national cyber resilience. The participation of critical economic sectors and sub-sectors from the economy and the corresponding CI operators is crucial to implementing the defined measures. The relevant federal offices must therefore ensure that these are successfully incorporated into the corresponding measures by means of a suitable information and consultation process. Criteria for the allocation of competencies can be found in the SKI strategy.

3.3 Subsidiary Role of the Armed Forces

Although the NCS explicitly excludes the case of war and conflict and instructs the armed forces to prepare themselves for such special cases, the armed forces do have extensive know-how regarding the technical aspects of cyber risks. The responsible office should be able to integrate and call upon these skills in their implementation processes. This is in keeping with the armed forces' traditional subsidiary role in the case of, for example, natural catastrophes. Initially, therefore, the skills and know-how in cyber risks should be built up or developed within the offices and areas of administration responsible for NCS implementation, calling upon the armed forces' skills and know-how in a targeted, solution-oriented manner. Through early coordination with NCS implementation, the offices responsible can thus identify and benefit from synergies in these areas. Correspondingly, early incorporation should also mean that the armed forces' future cyber defence plan can be aligned with the overall plan for Switzerland.

3.4 NCS Implementation Project Risks

Certain risks need to be taken into account when implementing the strategy. One of the greatest risks by far is that the implementation measures will fail to take effect in good time. Others include:

- risks caused by knowledge gaps among the individual players and incidents occurring before the strategy takes effect, making the strategy appear obsolete in the public mind;
- the risk and vulnerability analysis and continuity management could be compromised if the federal offices do not include the sectors/sub-sectors and the CI operators in time or to a sufficient extent;
- cooperation could be jeopardised by insufficient communication and unrealistic expectations on the part of the sectors/sub-sectors and the CI operators;
- failure to build up the necessary resources in good time could threaten implementation of the measures in all areas of the strategy;
- following implementation of the strategy, certain critical infrastructures may require further action, resulting in additional costs to deal with the corresponding risks.

4 Organisation of NCS Implementation

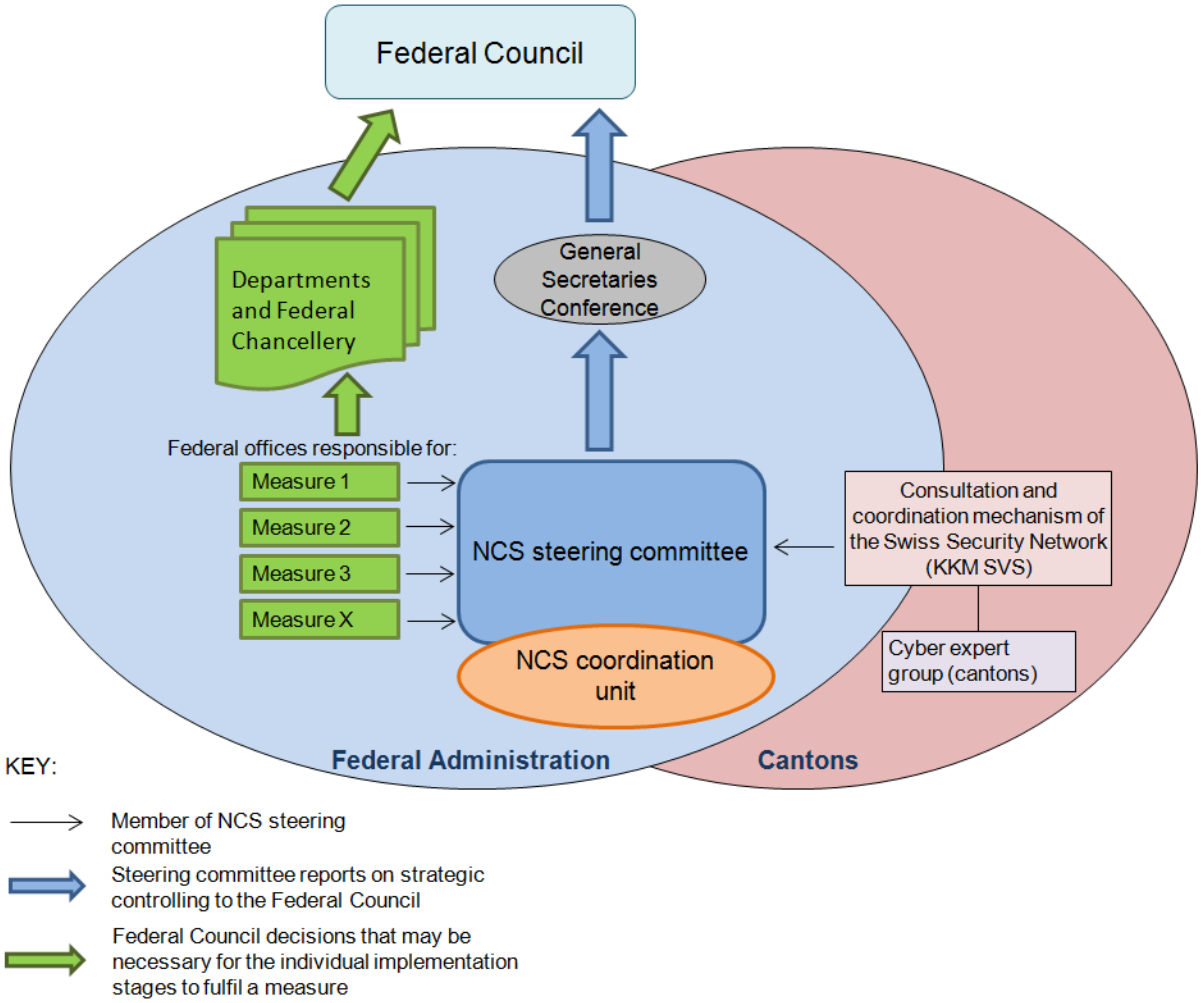

Figure 2: Organisation of NCS Implementation

4.1 NCS Steering Committee

The NCS steering committee is mandated by the Federal Council to secure the coordinated, purposeful implementation of the national strategy for the protection of Switzerland against cyber risks (see Figure 2).

Its roles and responsibilities are as follows:

- It uses strategic controlling tools to check that the portfolio of measures under the strategy is progressing as planned and on time and reports its findings to the Federal Council by way of the General Secretaries Conference.
- It ensures coordination among the relevant federal departments in implementation of the measures, particularly where these overlap with areas of legislation.
- It actively supports cooperation between the federal offices and the relevant bodies in the cantons, the private sector and civil society.

- It ensures that the activities for implementation take account of the Confederation's risk policy, the national strategy for protection of the critical national infrastructure and the Federal Council's strategy for an information society in Switzerland.
- It examines possible synergies with the responsible bodies and also the possibility of simplifying and streamlining the reporting paths and systems.
- It monitors developments regarding cyber risks and submits recommendations in this respect to the Federal Council for the further development of the strategy.
- It provides the Federal Council, via the Federal Department of Finance (FDF), with an annual report on the status of implementation of the strategy. At the end of 2017, it will submit a detailed final report with an assessment of the effectiveness of the strategy and its implementation plan. The assessment of effectiveness will be presented to the Federal Council already in the spring of 2017.

The steering committee includes representatives of all federal government departments with lead responsibility for implementing at least one of the measures. The consultation and coordination mechanism of the Swiss Security Network (KKM SVS) is also represented on the steering committee. The FDF holds the chair.

4.2 NCS Coordination Unit

The NCS coordination unit coordinates implementation of the strategy at an operational and technical level.

Its tasks are as follows:

- It systematically observes and evaluates the progress made in implementation and reports this back to the steering committee.
- It coordinates and supports the implementation activities of the offices responsible and carries out measures assigned to it.
- It identifies and utilises synergies between the implementation measures.
- It organises the cooperation among internal and external experts and with their organisations.
- It monitors national and also, in agreement with the Federal Department of Foreign Affairs (FDFA), international developments in matters related to cyber strategies and their implementation and reports its findings in good time to the relevant implementation partners.
- It holds an annual NCS expert event at which the implementation partners from all over Switzerland can meet up and share their know-how and information.

4.3 Cyber Expert Group and International Cyber Expert Group

To coordinate activities overlapping with the cantons, the consultation and coordination mechanism of the Swiss Security Network (KKM SVS) is setting up the cyber expert group with federal, cantonal and municipal representatives.

The cyber expert group coordinates NCS implementation at cantonal level. Its tasks are as follows:

- As the Confederation's key partner, it includes the cantons in all implementation measures concerning them.
- It manages sub-projects in the form of working groups in "Strengthening Resilience", "Incident Handling" and "Crisis Management".
- It coordinates implementation of the cantonal sub-projects and uses strategic controlling tools to check these are progressing as planned and on time.
- It ensures that members of the expert group are fully aware of the Confederation's implementation tasks in the strategy and fosters an exchange of experience between its members.

The NCS coordination unit is a member of the KKM SVS cyber expert group and forms the link at federal level to the cyber expert group's project work, so as to optimise synergies and prevent duplication of efforts.

There are also plans to create an international cyber expert group, under the FDFA, to secure the flow of information in close cooperation/coordination with all those involved. Parties expressing an interest in international cooperation in cyber security will be invited by the FDFA to attend a constituent meeting. This first meeting will discuss how participants could benefit from an inter-departmental working group dealing exclusively with the international aspects of cyber security.

5 Measures and Responsibilities

The seven spheres of action with the sixteen individual action points (measures) (M1-M16) can be broken down, in terms of timing and dependencies, into the following four areas:

- **Prevention**
- **Response**
- **Continuity and Crisis Management**
- **Supporting Processes**

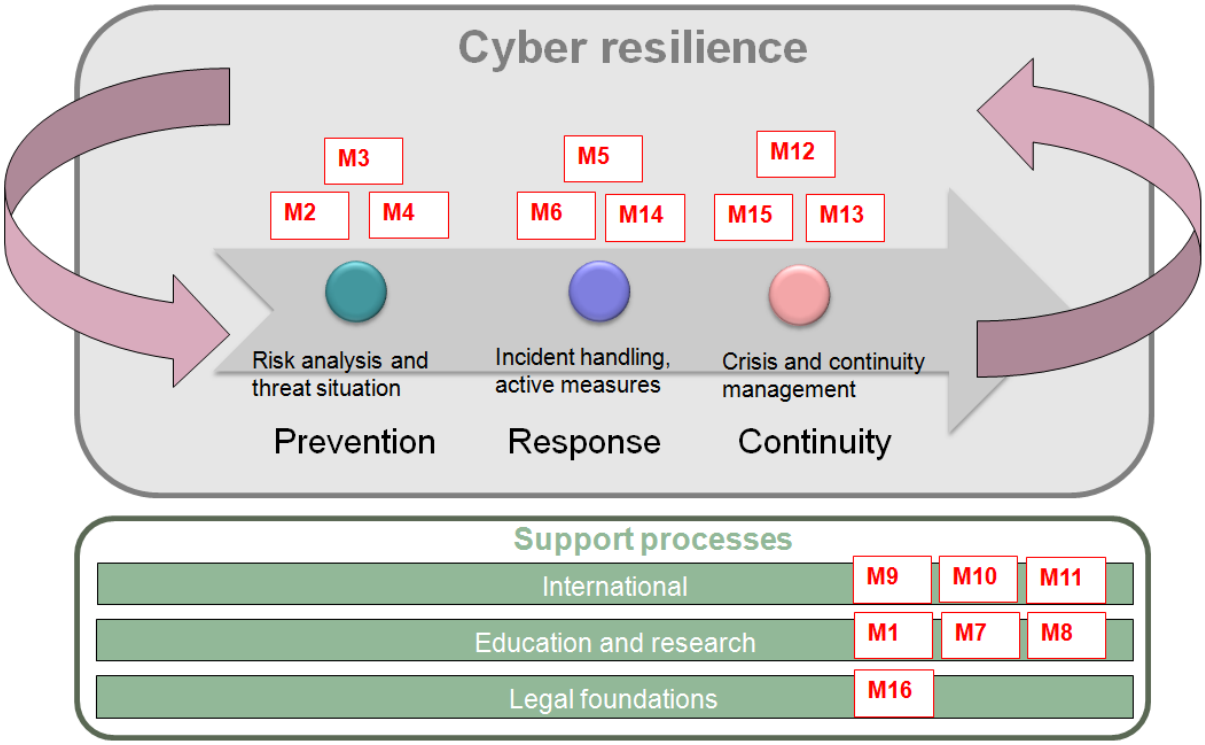

Figure 3: NCS strategy at a glance

Cyber resilience encompasses a set of recurrent processes of prevention, response and continuity. After the crisis management stage once an incident has occurred, the process starts again from the beginning.

The following sections present the key findings from interviews with the various players, according to the different areas and measures as well as their responsibilities, competent bodies, objectives in implementation and delivery deadlines.

5.1 Prevention

In terms of prevention, the overall risk management approach taken in the SKI strategy also applies with regard to cyber risk in the NCS strategy. The offices responsible for implementation have a risk and vulnerability analysis drawn up. This is primarily done under the leadership of the FONES and the competent authorities and regulators.

With regard to presenting the overall threat situation, information of both a technical and non-technical nature must be assimilated to ensure a complete analysis and evaluation of cyber risks. This information is made available by MELANI. Consequently, MELANI should be expanded to become the central information hub for the cantons and CI operators.

It can be assumed that most critical sectors/sub-sectors and the corresponding CI operators already systematically conduct a risk and vulnerability analysis. Given the increasing threat, the strategy must ensure that cyber security is explicitly addressed in the overall risk analysis. The NCS strategy recommends taking a uniform approach to this and compiling the consolidated results in the form of the current state poistion and its possible developments.

This approach should also ensure that cyber risks are disclosed in a transparent manner, specifically in the case of CI operators. Therefore, based on higher-level and national considerations, any unacceptable residual risk can be noted, and the costs incurred for the required action identified.

Sphere of action 2	**Competent bodies: FONES, FOCP, competent authorities/ regulators;** MELANI	**Measure 2**
Risk and vulnerability analysis	The FONES draws up the risk and vulnerability analysis together with the sectors/sub-sectors and CI operators. Sectors/sub-sectors not covered by the FONES should be addressed by the FOCP in collaboration with the competent authorities. The allocation of sub-sector responsibilities between the FONES and the FOCP is clearly defined.	Independent evaluation of systems. Risk analyses to minimise risks in collaboration with authorities, ICT service providers and system suppliers.

Implementation:

The FONES[3] and the FOCP[4] are charged with compiling a risk and vulnerability analysis for their respective sub-sectors. Wherever possible and relevant, the FONES and the FOCP should agree upon the procedure and the methods to be used. Sectors/sub-sectors not covered by the FONES should be addressed by the FOCP with the collaboration of the competent authorities (the regulators responsible). The approach adopted should be as consistent as possible. The work should be completed by end-2017.

The results are consolidated in cooperation with MELANI to form a comprehensive analysis of the threat situation.

[3] See footnote 1
[4] See footnote 2

Sphere of action 2	**Competent bodies: FITSU;** FOITT, CSO, MELANI	**Measure 3**
Risk and vulnerability analysis	Together with the ICT service providers, the FITSU draws up guidelines, designed for testing vulnerabilities (*Prüfkonzept*). This may serve as a supplement to the SKI guidelines on cyber security. MELANI coordinates the exchange of information with the CI operators, ICT services providers and system suppliers.	The ICT infrastructure should be tested for systemic, organisational and technical vulnerabilities. The authorities, CI operators and research institutions examine their ICT infrastructure for vulnerabilities in collaboration with the ICT service providers and system suppliers.

Implementation:

The Security department at the FITSU (FITSU-SEC) draws up such guidelines by end 2015 to be implemented by the relevant service providers and those responsible within the General Secretariats of federal government departments. The Federal Office of Information Technology, Systems and Telecommunication (FOITT) and the Armed Forces Command Support Organisation (CSO) support these guidelines as ICT service providers. These guideline may be issued as a recommendation to the private sector and the CI operators. It may also be presented to the cantons by the KKM SVS cyber expert group and thereby serve as a recommendation and support for their own evaluation.

The guidelines will be coordinated with ongoing projects, such as Information Security Management Systems (ISMS) by Information Security and Facility Protection (ISFP).

The results are consolidated in collaboration with MELANI to form a comprehensive analysis of the threat situation.

Sphere of action 3	**Competent bodies: MELANI, FIS, CYCO;** CSO, MIS, FOITT	**Measure 4**
Analysis of the threat landscape	Intelligence, police, forensic and technical information is obtained from open and classified sources about cyber threats and the risk situation. This measure is implemented in various projects with different lead bodies. MELANI works in close cooperation with the FIS and fedpol/CYCO to generate an image of the current threat situation. The Federal Intelligence Service (FIS) covers the cyber-related aspects of its remit. CERTs: Technical capacities to be built up to provide 24/7 surveillance: CSIRT-FOITT, FIS-CSIRT, GovCERT.	Establish a picture of the overall situation and its development

Implementation:

MELANI: Creation (by end-2013) and implementation (starting in 2014) of a plan to reinforce MELANI as an information exchange platform. MELANI strengthens the systematic cooperation with relevant ICT service providers and system suppliers. Increased information exchange with the CI operators and the private sector.

FIS**:** Specialist knowledge and skills related to cyber security to be built up at the FIS, with CSO-EOC and the Military Intelligence Service (MIS) as service providers for the FIS (2014-2015).

The technical capacities for 24/7 surveillance should be built up by end-2015.

- CERTs: MELANI**:** Expansion of GovCERT to increase resilience (2014-2016)
- FOITT: Expansion of the CSIRT to increase detection capacity

5.2 Response

The NCS action points (measures) for incident handling and incident response are aimed at strengthening existing tasks and capacities that contribute to cyber resilience and cannot be performed by individual players alone. In the course of incident handling and incident response, the need for specific active countermeasures may also arise. Ultimately, the extent to which Switzerland should be able to take active measures in other countries below the threshold of war should be determined within the political decision-making process.

Sphere of action 3	**Competent bodies: MELANI, FIS;** CSO, MIS, FOITT	**Measure 5**
Analysis of the threat landscape	The federal administration, the cantons and CI operators should review relevant incidents and evaluate possibilities of developing their own measures for tackling incidents in relation to cyber risks. MELANI gathers, evaluates and analyses the findings and makes these available to the relevant players (PPP Model). FIS remit, as in M4.	Review of incidents for the development of measures.
Implementation: As in M4. FOITT: Expansion of technical capacities (improve ability to respond to an incident) to enable 24/7 surveillance. The CSIRT-FOITT should be expanded to strengthen technical capacity and resilience by 2014. This expansion can also support M4.		

Sphere of action 3	**Competent bodies: CYCO;** MELANI	**Measure 6**
Analysis of the threat landscape	The cantons are directly responsible for prosecution in the case of cyber-related incidents.	Case overview and coordination of inter-cantonal clusters of cases.

Implementation:

In collaboration with the cantons, fedpol draws up a plan to manage a comprehensive overview of cases (offences) and to coordinate inter-cantonal clusters of cases. This plan is subject to two consultation processes in the cantons and is approved by the Conference of Cantonal Justice and Police Directors (KKJPD). Within fedpol CYCO is in charge of overall coordination. The plan should pay particular attention to existing projects between the cantons and the Confederation (e.g. harmonisation of police information technology (HPI); plan to create a case overview in the area of burglary crime). A core group for project organisation is to be defined in Q2 2013. This will comprise representatives of:

Fedpol, KKJPD, Conference of Law Enforcement Authorities of Switzerland (KSBS), Conference of Cantonal Police Commandants of Switzerland (KKPKS), Head of IT working group of KKPKS, representatives of Swiss Police ICT, a representative of the Office of the Attorney General (BA) and the Federal Office of Justice (BJ).

The first consultation process will be held in Q2 2014 and the second in Q4 2014. The plan should be drawn up and ratified by the KKJPD by Q3 2015. The internal consultations then begin in Q4 2015. Preparations for implementation will follow in 2016.

At an international level, Europol and Interpol are the main players with whom the plan must be coordinated.

The information obtained from the overview of cases (offences) and findings concerning clusters of cases from the technical/operational analysis of prosecution will flow into the overall analysis of the threat situation via MELANI.

Sphere of action 6	**Competent bodies: FIS, MELANI;** CYCO, MIS	**Measure 14**
Continuity and crisis management	The FIS is in charge of information gathering through its intelligence channels, in order to analyse and evaluate this information and subsequently disseminate the results. In collaboration with the CSO as its technical service provider and the MIS as its interface to military intelligence, it builds capacities to identify the perpetrator(s) and prepares active measures in the case of political expediency. CYCO (fedpol) also plays an important role in the prosecution and identification of perpetrators. CYCO will be called upon accordingly.	Active measures to identify the perpetrator(s). If the FIS manages to identify the perpetrator(s), it forwards the corresponding information, as long as it is legally permissible, to the Office of the Attorney General, which decides whether to institute criminal proceedings. If prosecution is not appropriate or not possible, active countermeasures should be prepared. The corresponding legal basis should be provided for in the Intelligence Services Act.
Implementation: Amendment of the SLA (Service Level Agreement) with CSO-EOC by end-2013. Specialist knowledge to be built up at the FIS, with CSO-EOC and the MIS as service providers for the FIS (2014-2015). The findings of the threat situation analysis by MELANI and the possibilities inherent in the legal remit for criminal prosecution of identifying and condemning the perpetrator influence the measures.		

5.3 Continuity and Crisis Management

The state is expected to have the means to provide subsidiary support to the responsible bodies if these are no longer capable of taking the necessary measures themselves. Together with its suppliers (particularly the FIS), MELANI provides such support to members of its closed user group (CUG). These services should be incorporated into all sectors/subsectors and all CI operators.

The processes for incident analysis and for continuity and crisis management must be closely coordinated with each other. As a rule, it can be argued that a crisis is triggered by an incident, but not every incident develops into a crisis. Escalation processes are therefore necessary from incident handling to crisis management. Crisis management plans form part of continuity management. The relevant offices and also the competent authorities and regulators should therefore ensure for their own area of responsibility that the sectors and subsectors and the corresponding CI operators have a functioning incident handling and crisis management system.

Sphere of action 6	**Competent bodies: FONES, FOCP, competent authorities/regulators;** MELANI	**Measure 12**
Continuity and crisis management	The competencies for continuity management are the same as for M2.	Strengthening and improving resilience towards disturbances and incidents.
Implementation: Implementation of continuity management is the same as in M2. The EAER is thus adapting its competencies in this respect as part of the NESA revision. Continuity management is an ongoing process. As it is based on the existing risk and vulnerability analyses, it can only be conducted once M2 has been completed. MELANI supports and reinforces the voluntary mutual exchange of information with CI operators, ICT service providers and system suppliers in support of continuity and resilience on the basis of self-help. This leads to a greater need for forensic capabilities and an increasing flow of information.		

Sphere of action 6	**Competent bodies: FONES, MELANI, FOCP;** CYCO, FDFA, competent authorities/ regulators	**Measure 13**
Continuity and crisis management	The competencies for crisis management are the same as for M2 and M12. MELANI takes charge of operational aspects and, in a crisis situation, provides subsidiary support to those affected by making the relevant expertise available. Fedpol/CYCO are closely involved in order to secure the prosecution. In cases with possible foreign-policy implications, the FDFA should be informed as early as possible and included in the preventative planning. The lead offices work in coordination with each other.	Coordination of activities, primarily with those directly involved, and support of decision-making processes with the relevant expertise.

Implementation:

Implementation of crisis management is the same as in M12. The EAER is therefore seeking to adapt its competencies in this respect as part of the NESA revision. Crisis management is an ongoing process. As it is based on the existing risk analyses, it can only be conducted once M2 has been completed.

MELANI and its partners in its closed user group create functional processes to deal with escalating incidents with the existing crisis organisations in public administration and the private sector.

A coordinated approach between the FONES and the FOCP is important in order to ensure a uniform and systematic procedure and take advantage of the existing contacts.

Sphere of action 6	Competent body: Federal Chancellery	Measure 15
Continuity and crisis management	Under the supervision of the Federal Chancellery, a plan should be drawn up for management procedures and processes on timely problem-solving that also addresses cyber-specific aspects.	Formulation of a plan for management procedures and processes for timely problem resolution.
Implementation: The (general) crisis management plan must be adapted and also include cyber-specific aspects. The Confederation's management procedures and processes address cyber-specific aspects within existing processes. Under the supervision of the Federal Chancellery, a plan should be drawn up for management procedures and processes on timely problem-solving that also addresses cyber-specific aspects.		

5.4 Supporting Processes

As the protection of information and communication infrastructure from cyber threats lies in Switzerland's national interest, the necessary basis for this must be created. This includes:

- checking whether existing legislation allows for these security measures,
- international cooperation and efforts to prevent cyber crime through internationally agreed rules and standards,
- exchanging experience, R&D findings, incident-specific information as well as training and exercises,
- participation by Switzerland in international government and non-government organisations for the reduction of cyber risks.

In order to increase cyber resilience, individual bodies must be able to identify, evaluate and analyse risks associated with cyber security in their own area of responsibility. The NCS strategy thus instructs the competent federal offices to implement the following measures, some of which they will tackle in association with the competent cantonal bodies. Cantons and CI operators must be able to rely on this basis to strengthen cyber resilience, as these are government tasks that cannot be performed by individual players alone.

Sphere of action 1	**Competent bodies: Responsible federal offices**	**Measure 1**
Identification of risks through research	To be clarified in the course of further implementation.	New risks in connection with cyber crime will be researched.

Implementation:

The following stakeholders may identify knowledge and skill gaps in cyber security:

- CERTs
- CI operators
- ICT providers

The following have research projects or programmes in the field of cyber security:

- EU
- Departments of the Federal Institutes of Technology (ETHZ/EPFL)
- Universities and technical colleges
- ICT research labs (e.g. IBM)

Sphere of action 4	**Competent bodies: NCS coordination unit;** OFCOM, FDFA, FSIO	**Measure 7**
Competence building	In collaboration with the FSIO (Youth and Media),[5] the FDFA and OFCOM, the NCS coordination unit compiles an overview of competence building offers. This overview is drafted in coordination with implementation of the "Federal Council's strategy for an information society in Switzerland" and the cantons. The FDFA provides information on offers concerning international organisations and institutions.	Establish an overview of existing competence building offers.

Implementation:

The overview of existing competence building offers should be completed by end 2013 and published by mid 2014.

[5] BRB 11.06.2010, National programme for youth media protection and media competencies.

Sphere of action 4	**Competent bodies: NCS coordination unit;** OFCOM, FDFA, FSIO	**Measure 8**
Competence building	In agreement with the Federal Council's strategy for an information society in Switzerland, the cantons and the private sector, in collaboration with the FSIO, FDFA, OFCOM and the authorities and regulators concerned, the NCS coordination unit coordinates the drafting of an implementation plan. This plan foresees the increased utilisation of existing “best practices” in education with regard to cyber risks and for creating new formal and informal options for competence building offers. The FDFA provides information on offers concerning international organisations and institutions.	Filling of gaps in competence building offers and increased utilisation of “best practices”.
Implementation: An implementation plan on increased utilisation of existing options in dealing with cyber risks and new competence building opportunities should be created by end-2015.		

Sphere of action 5	**Competent bodies:** **OFCOM;** competent authorities/regulators, FDFA, SECPOL, MELANI	**Measure 9**
International relations and initiatives	OFCOM participates actively in relevant international processes and institutions in relation to Internet governance (particularly ICANN, ITU, CSTD and IGF). It identifies on an ongoing basis those aspects of relevance to Internet stability, availability and security, coordinates Swiss interests with representatives from public administration, the private sector and civil society, and defends these interests in the aforementioned processes and institutions.	Internet governance: Switzerland actively advocates a coordinated Internet governance that is compatible with the Swiss concept of freedom and (personal) responsibility, basic supply, equal opportunities, human rights and the rule of law.
Implementation: OFCOM and the FDFA, with the support of the DDPS for issues of security policy (GS-DDPS/SECPOL), compile by end-2013 an overview of priority events, initiatives and international committees concerning Internet governance, in collaboration with the federal departments involved.		

Sphere of action 5	**Competent bodies: FDFA;** SECPOL, MELANI, OFCOM	**Measure 10**
International relations and initiatives	The FDFA should set specific activities in motion in international cooperation. One possibility is to establish a code of conduct for cyber-related aspects. The long-term objective is to establish internationally binding guidelines. The possibility of making Geneva a central hub for Internet issues is being examined. The FDFA is supported in the implementation of this measure by GS-DDPS/SECPOL.	Cooperation at the international security policy level, in order to address the threat in cyber security together with other countries and international organisations. Specific activities should be set in motion or existing ones continued in order to allow Switzerland to defend its interests within the various international committees.
Implementation: An FDFA-internal medium-term plan for NCS implementation in international cooperation should be drawn up by end-2013. This process is supported by MELANI and OFCOM.		

Sphere of action 5	**Competent bodies: NCS coordination unit;** competent authorities/ regulators, FDFA, MELANI	**Measure 11**
International relations and initiatives	MELANI and the competent authorities and regulators reinforce the exchange of information among CI operators, ICT service providers and system suppliers on international approaches and initiatives. MELANI and DETEC thus promote the coordinated influence of Switzerland as an economic centre in these international panels. If desired, MELANI, DETEC and the FDF ensure such participation in agreement with the federal departments, particularly the FDFA.	Coordination of those involved in initiatives and "best practices" relating to security or assurance processes. Within the context of private and national initiatives, conferences and standardisation processes related to security and assurance, the operators, associations and authorities coordinate their efforts to influence these panels.
Implementation: In the initial stage, the partners involved (competent authorities and regulators) should draw up a list of those who should normally participate in international initiatives and committees. This list should be consolidated in a second stage, to include authorities, industry and possibly also the FDFA. This process is coordinated by the NCS coordination unit..		

Sphere of action 7	**Competent bodies: NCS coordination unit**	**Measure 16**
Legal basis	The FITSU coordinates this measure with the relevant federal departments. For legislative gaps that have been identified as priorities and the necessary legal adjustments, the relevant federal departments will draw up the corresponding drafts on the appropriate standard basis.	Evaluation of existing legislation.
Implementation: In collaboration with the federal departments, the NCS coordination unit will draw up by end-2013 an initial overview of urgent legislative and revision requirements regarding cyber security. For those legislative gaps identified as priorities, the Federal Council must be presented with a regulatory plan including a timetable by end 2014 at the latest.		

6 Annex

Referenced Documents

Title	Author/ publisher	Date
[1] National strategy for the protection of Switzerland against cyber risks	DDPS	19.06.2012
[2] National strategy for protection of critical infrastructure	DDPS - FOCP	27.06.2012
[3] Guidelines for protection of critical infrastructure	DDPS - FOCP	Draft 23.07.2012
[4] Handbook of risk management for the Confederation	FDF	Version 1.0

List of Interviewees

Federal offices	Participants	Date
CSO	Riccardo Sibilia, Gérald Vernez	11.01.2013
FDFA	Michele Coduri, Christoph Bühler	21.01.2013
fedpol-CYCO	Roland Becker, Thomas Walther, Tobias Bolliger	11.01.2013
FINMA	Marc Sander	04.01.2013
FIS	Philipp Kronig, Reto Camenisch	17.01.2013
FITSU-MELANI	Pascal Lamia, Stefanie Frey	18.01.2013
FITSU-SEC	Marcel Frauenknecht, Franz Zingg, Daniel Graf	11.01.2013
FOCA	Urs Haldimann	11.01.2013
FOITT	Heino Kronenberg	17.01.2013
FONES-FOCP-FITSU (coordination meeting)	Ruedi Rytz (FONES), Toni Lauber (FONES), Stefan Brem (FOCP), Nick Wenger (FOCP), Pascal Lamia (FITSU), Stefanie Frey (FITSU), Franz Zingg (FITSU), Marc Henauer (MIS)	07.01.2013
FOT	Petra Breuer, Ulrich Schär, Heinz Geiser	14.01.2013
FSIO	Thomas Vollmer	27.02.1013
GS-DDPS	Jürg Treichler	14.01.2013
KKM SVS	Bernhard Wigger, Dario Walder	14.01.2013
OFCOM	Armin Blum	17.01.2013
SFOE	Christian Holzner, Hans-Peter Binder	17.01.2013

Abbreviations

Abbreviation	Description
CERT	Computer Emergency Response Team
CI operator	Critical infrastructure operator
CSIRT	Computer Security Incident Response Team
CSO	Armed Forces Command Support Organisation
CSO-EOC	Electronic Operations Centre in the Armed Forces Command Support Organisation
CUG	Closed User Group (element of MELANI)
CYCO	Cybercrime Coordination Unit Switzerland within the FDJP
EFT	Education, Research & Technology
FITSU-SEC	IT security section of the Federal IT Steering Unit
FOITT	Federal Office of Information Technology, Systems and Telecommunication
FSIO	Federal Social Insurance Office
KKJPD	Conference of Cantonal Justice and Police Directors
KKM SVS	Consultation and coordination mechanism of the Swiss Security Network
KKPKS	Conference of Cantonal Police Commandants of Switzerland
KSBS	Conference of Law Enforcement Authorities of Switzerland
MELANI	Reporting and Analysis Centre for Information Assurance
MIS	Military Intelligence Service in the DDPS
NCS	National strategy for the protection of Switzerland against cyber risks
NCS coordination unit	Coordination unit for implementation of the NCS strategy
NESA	Federal Act of 8 October 1982 on the National Economic Supply (National Economic Supply Act, NESA)
SiLAN-FIS	Security LAN of the FIS
SECPOL	Security Policy (Organisational Unit in the GS-DDPS)
SKI strategy	National strategy for protection of critical infrastructure
SONIA	Special Task Force for Information Assurance