



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

Federal IT Steering Unit (FITSU)  
Federal Intelligence Service (FIS)

**Reporting and Analysis Centre for Information Assurance (IA)**

**MELANI**

# **National Strategy for the Protection of Switzerland against Cyber Risks**

**ITU Cybersecurity Workshop: Cybersecurity and Cyber Risk  
Assessment in Practice  
Geneva, 26 January 2017**

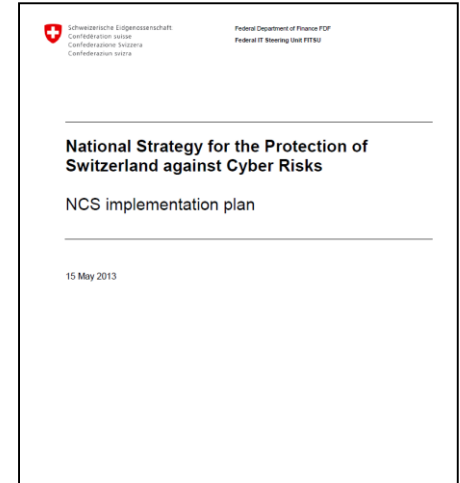
Stefanie Frey, Coordinator National Cyber Strategy (NCS), MELANI  
IA/FITSU, Federal Department of Finance (FDF)



# NCS and Cyber Risk Assessment



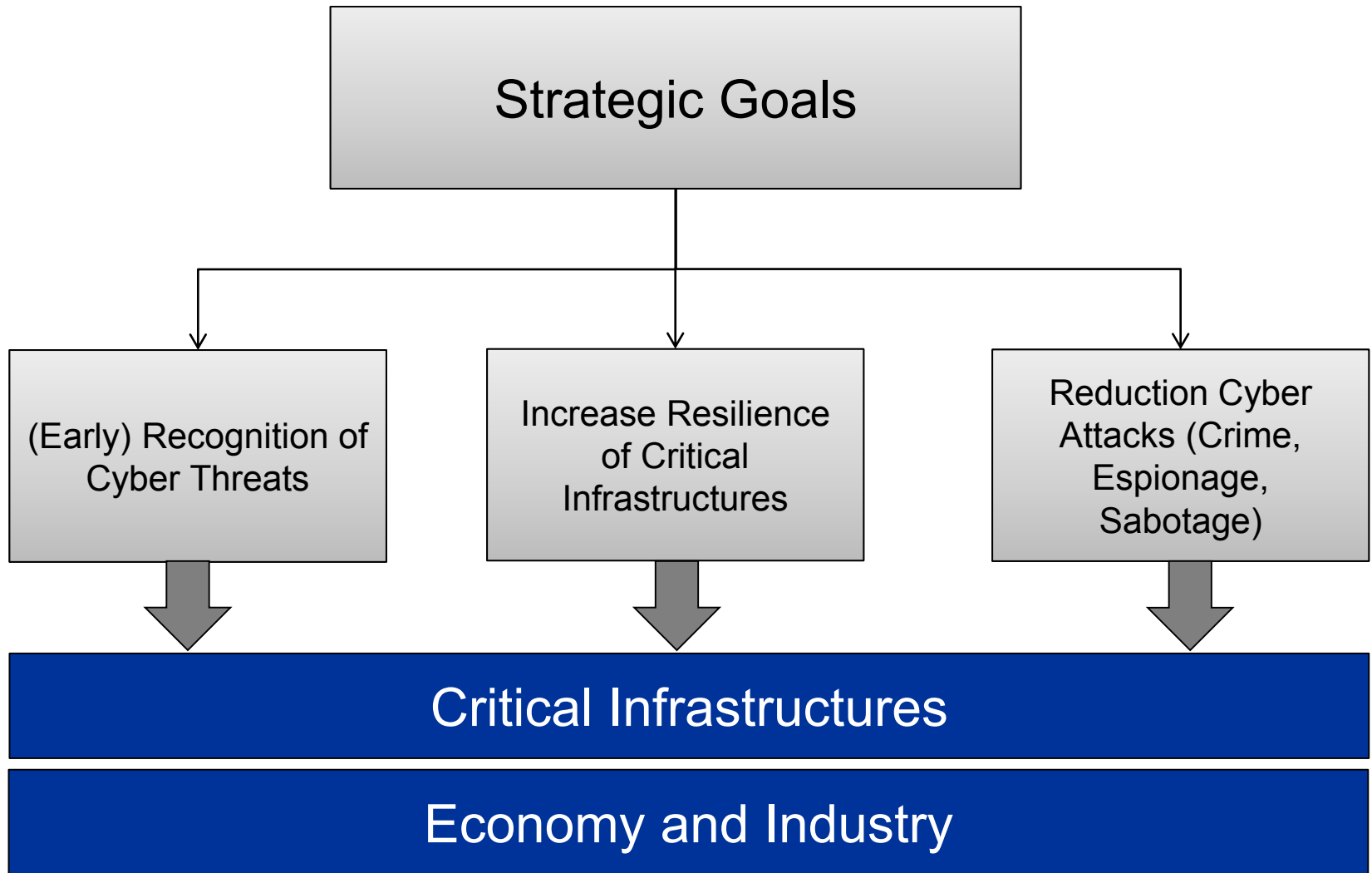
**National Strategy for Switzerland's protection against Cyber Risks (NCS)**  
7 Spheres of Action (16 Measures)



- Identification of ICT-Vulnerabilities
- Strengthened Resilience against Cyber Risks



# Strategic Goals





# 28 Critical Sectors and Sub-Sectors

<b>Critical Sectors</b>	<b>Public Administration</b>	Parliament, government, justice and administration
		Diplomatic Missions
		Research institutions
		Cultural properties
	<b>Energy</b>	Oil supply
		Natural gas supply
		Power supply
	<b>Waste disposal</b>	Waste
		Waste water
	<b>Finances</b>	Banks
	Insurances	
<b>Health</b>	Medical care and hospitals	
	Laboratories	
<b>Industry</b>	Chemistry and alternative medicine	
	Machine, electro industry	
<b>Information and communication technology</b>	Information technology	
	Media	
	Postal services	
	Telecommunication	
<b>Food</b>	Food supply	
	Water supply	
<b>Public safety</b>	Armed forces	
	Civil protection	
	First responders (police, fire services)	
<b>Transport</b>	Road transport	
	Rail transport	
	Air transport	
	Navigation	
	<b>Critical Sub-sectors</b>	

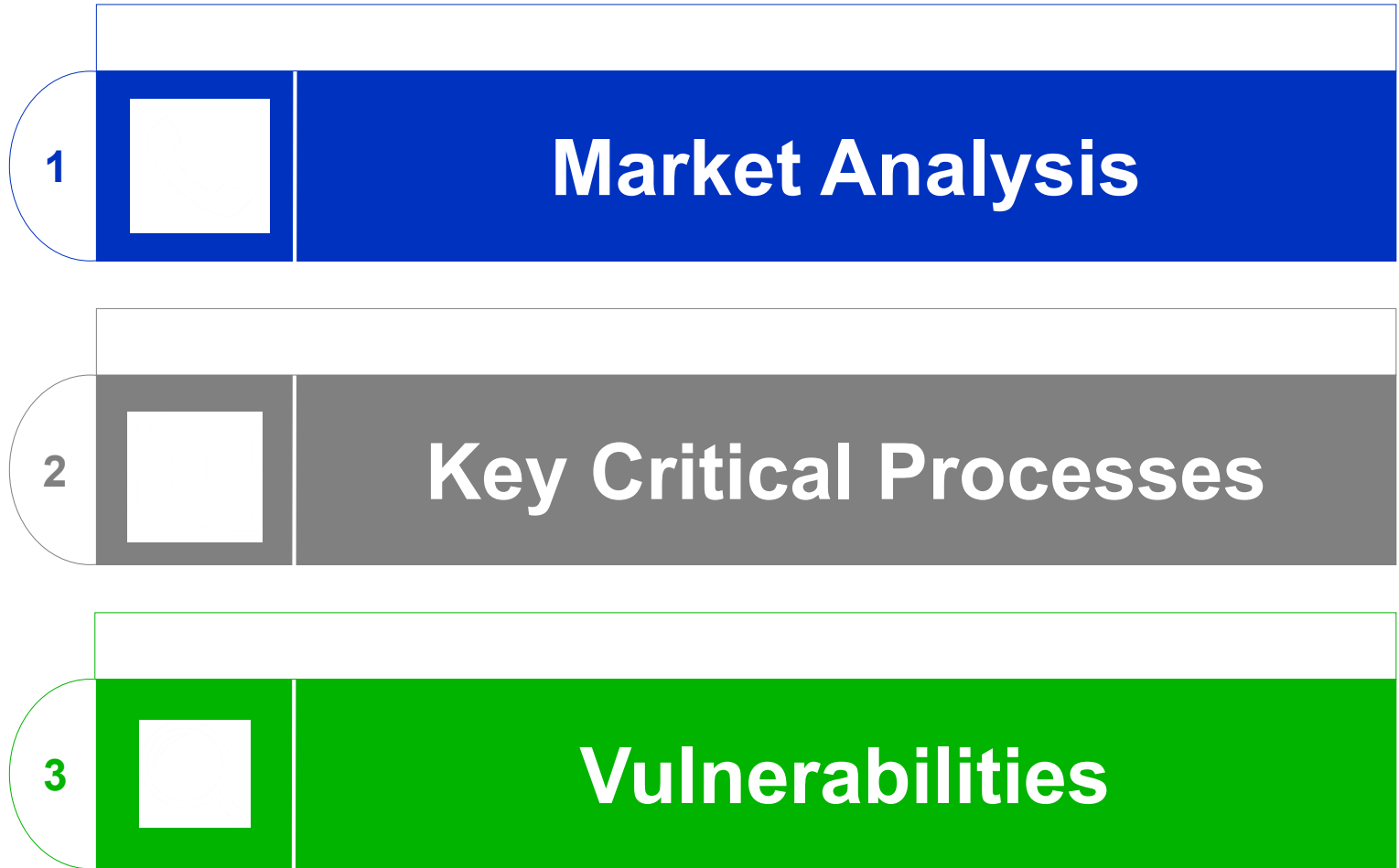
Source: National Strategy for the protection of critical infrastructures, FOPP



# Cyber Risk Assessment of CIIP



# Methodology





# Point of Departure

Focus on Vulnerability Assessment AND NOT Risk Assessment

1

**Classical Approach**

Risk

=

Likelihood of Occurrence

x

Extent of Damage

2

**Problem**



- Insufficient Information on likelihood of occurrence and extent of damage
  - Unknown vulnerabilities and a lack of information
  - Estimation of likelihood and extent of damage difficult
- **Quantitative approach not effective**

3

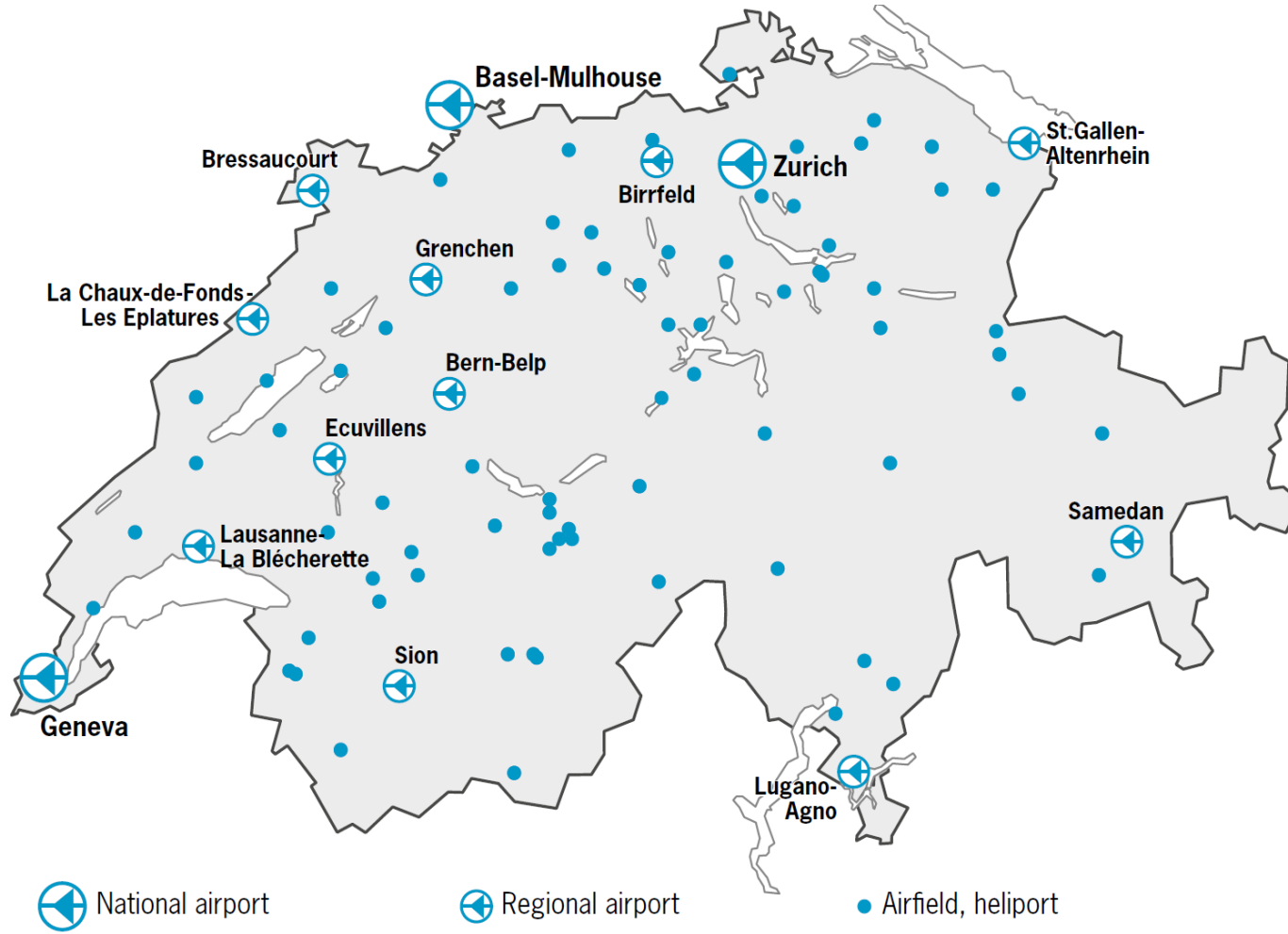
**Solution**

**Qualitative Approach**

Qualitative Analysis of Vulnerabilities and definition of suitable measures to improve security and resilience



# Swiss Aviation







# Vulnerability of processes

The vulnerability of processes and sub-processes was determined using the following weighted criteria:





# Thank You for Your Attention

Dr. Stefanie Frey  
Coordinator National Cyber Strategy NCS

Reporting and Analysis Centre for Information Assurance (MELANI)

Federal IT Steering Unit (FITSU)

Schwarztorstrasse 59  
CH-3003 Bern

Stefanie.frey@isb.admin.ch  
[www.melani.admin.ch](http://www.melani.admin.ch)