Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal IT Steering Unit FITSU
Federal Information Service FIS

Reporting and Analysis Centre for Information Assurance MELANI

The role of the Swiss Government in dealing with Cyber Incidents

Swiss Cyber Storm, Lucerne, 22 October 2014

Dr. Stefanie Frey, Coordinator Swiss National Cyber Strategy

MELANI: Information Exchange Hub

Responsibilities

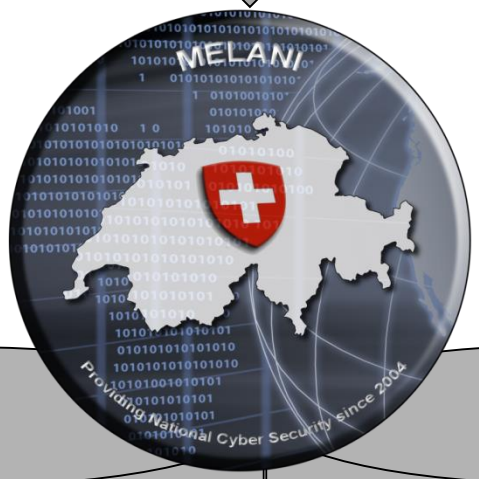
Operative Support

Closed Constituency: Critical Infrastructure Operators

Closed Constituency

Sectors:

- Chemistry/Pharmacy
- Energy
- Finance
- Health
- Industry
- Telecom
- Transport/Logistics
- Insurance
- Administration



Identification
Evaluation
Analysis

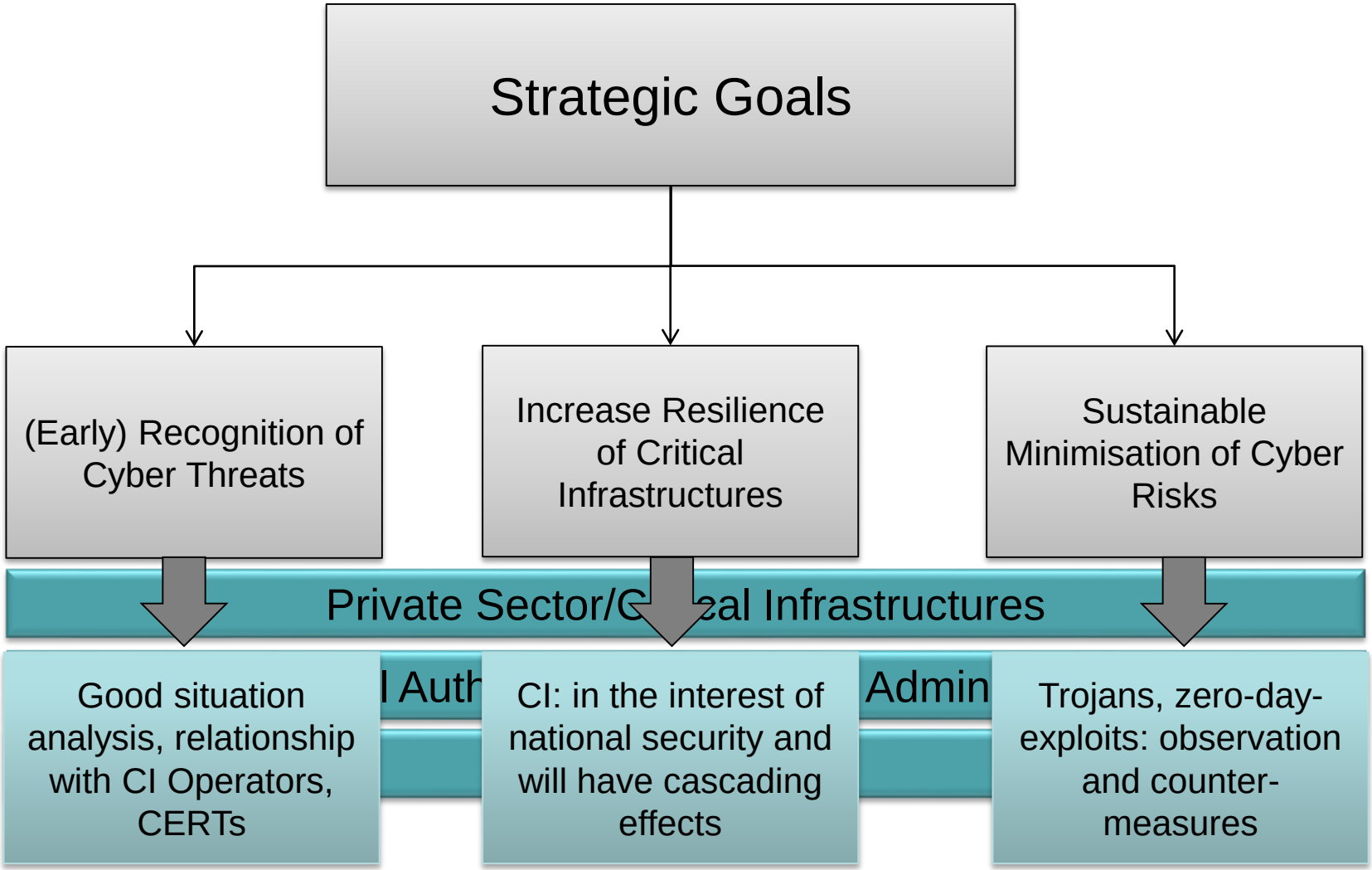
FIS – Intelligence Gathering and Analysis

Contact to Security Relevant Services

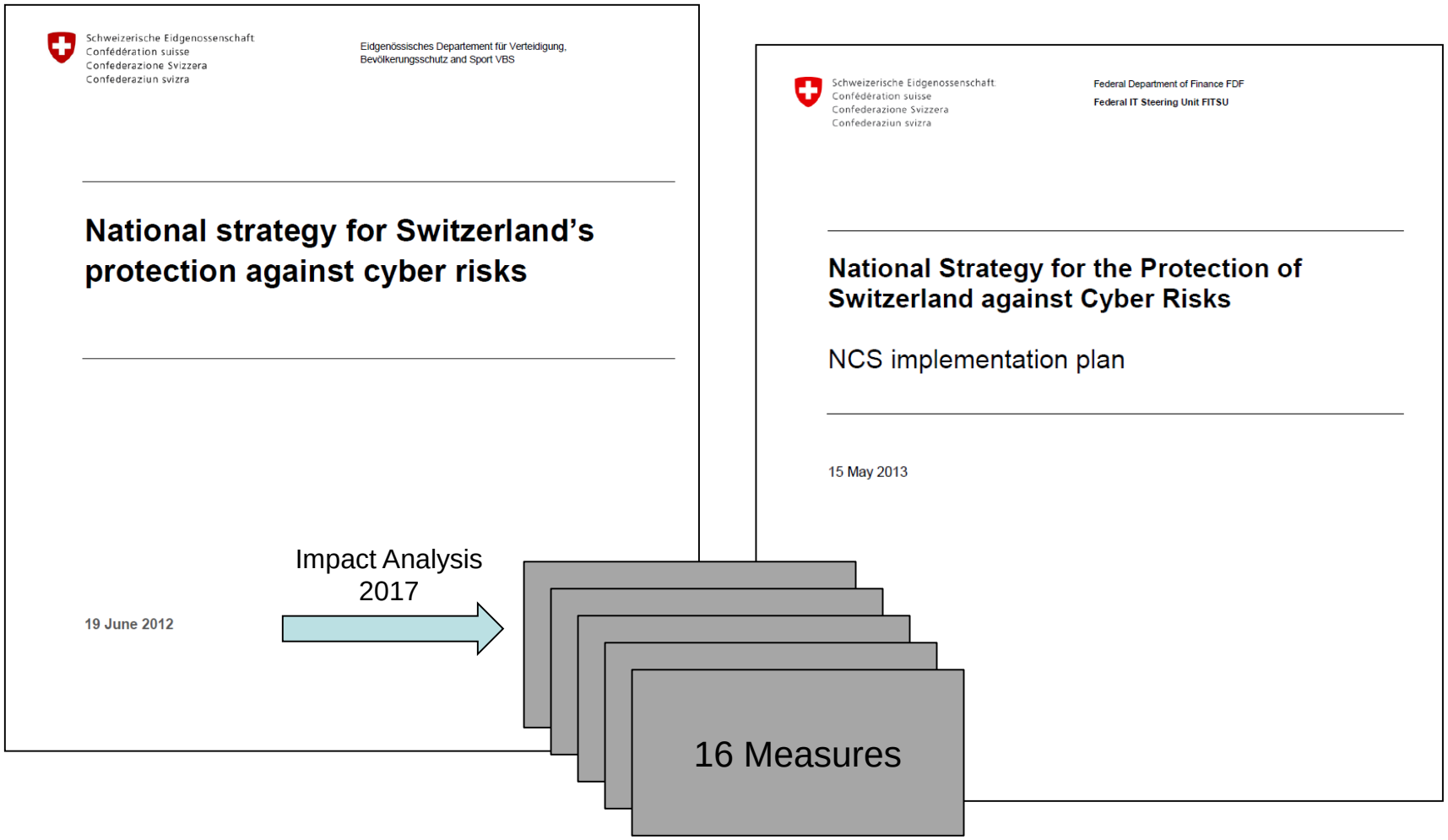
FITSU –Technological Centre of Competence

Contact to IT-Security Relevant Actors

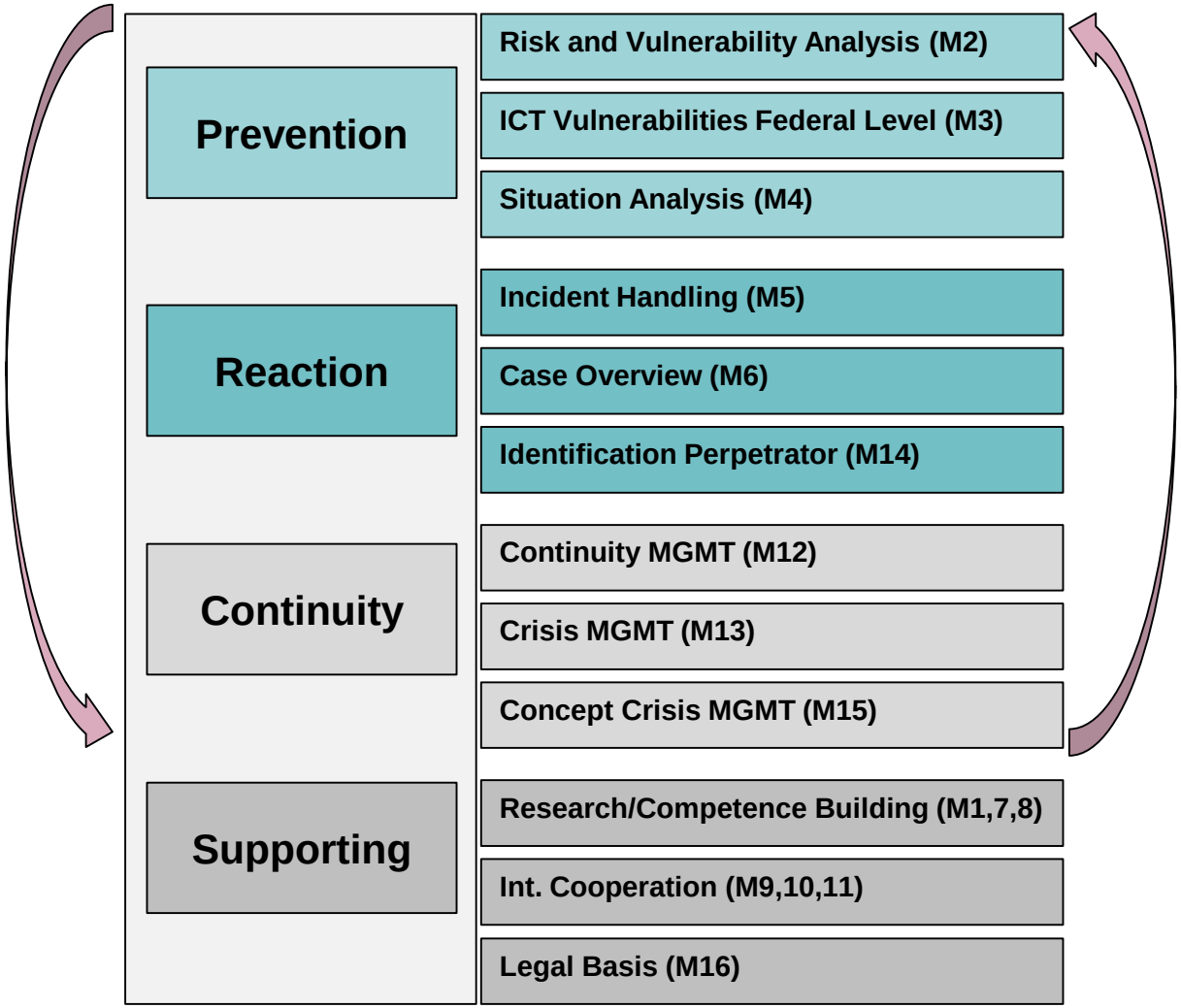
Strategic Goals



NCS: A comprehensive Strategy



Implementation and Responsibilities



Decentral Implementation: Individual Self Responsibility, State offers Subsidiary Support

Riskmanagement: Risk based approach, Cyber is part of the overall risk management

Flexibility: Customised solutions and technical and non technical solutions

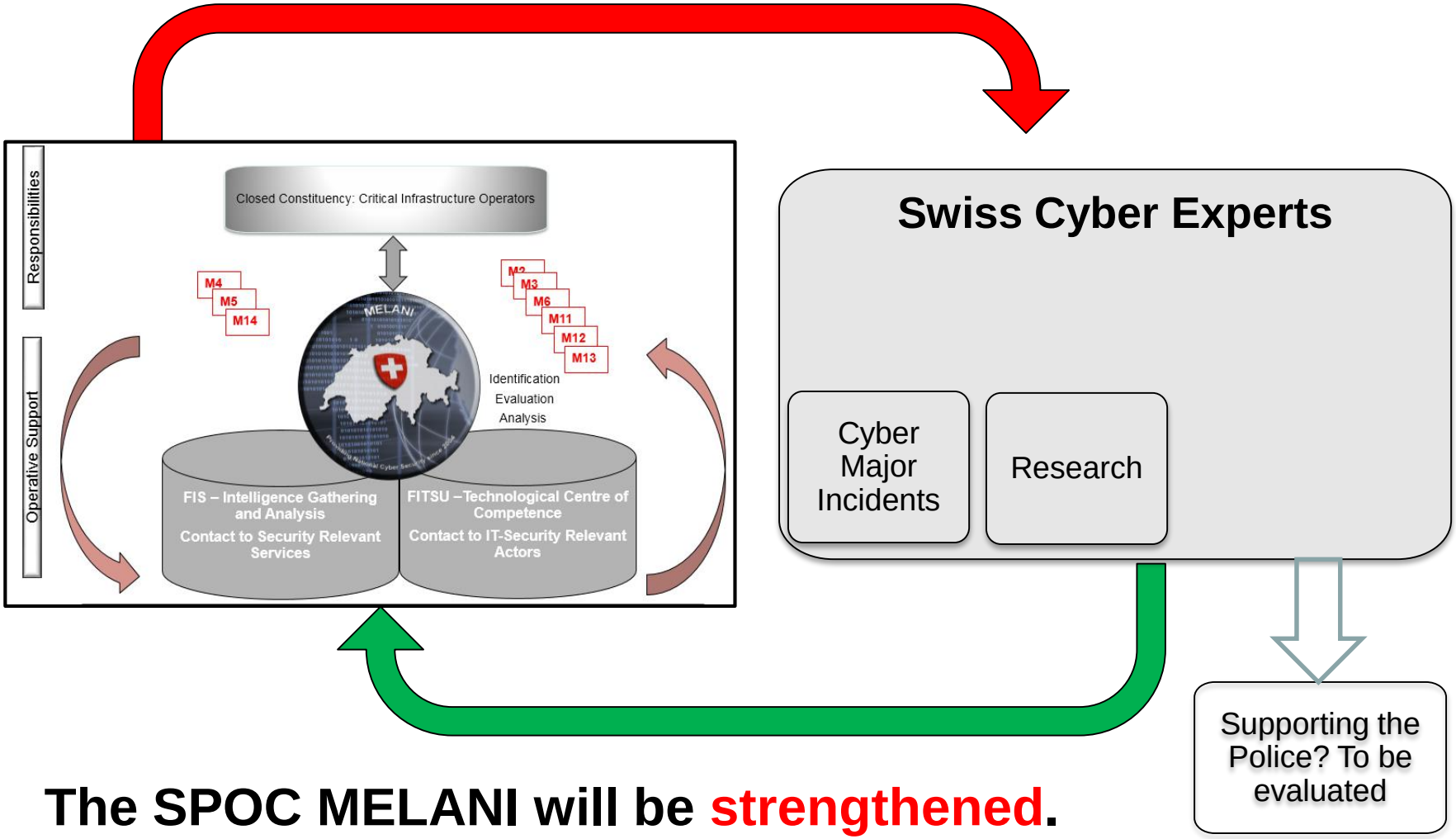
Swiss Cyber Experts

Incident Handling and Continuity MGMT

MELANI:
Public-Private- Partnership (PPP) and **Swiss Cyber Experts**

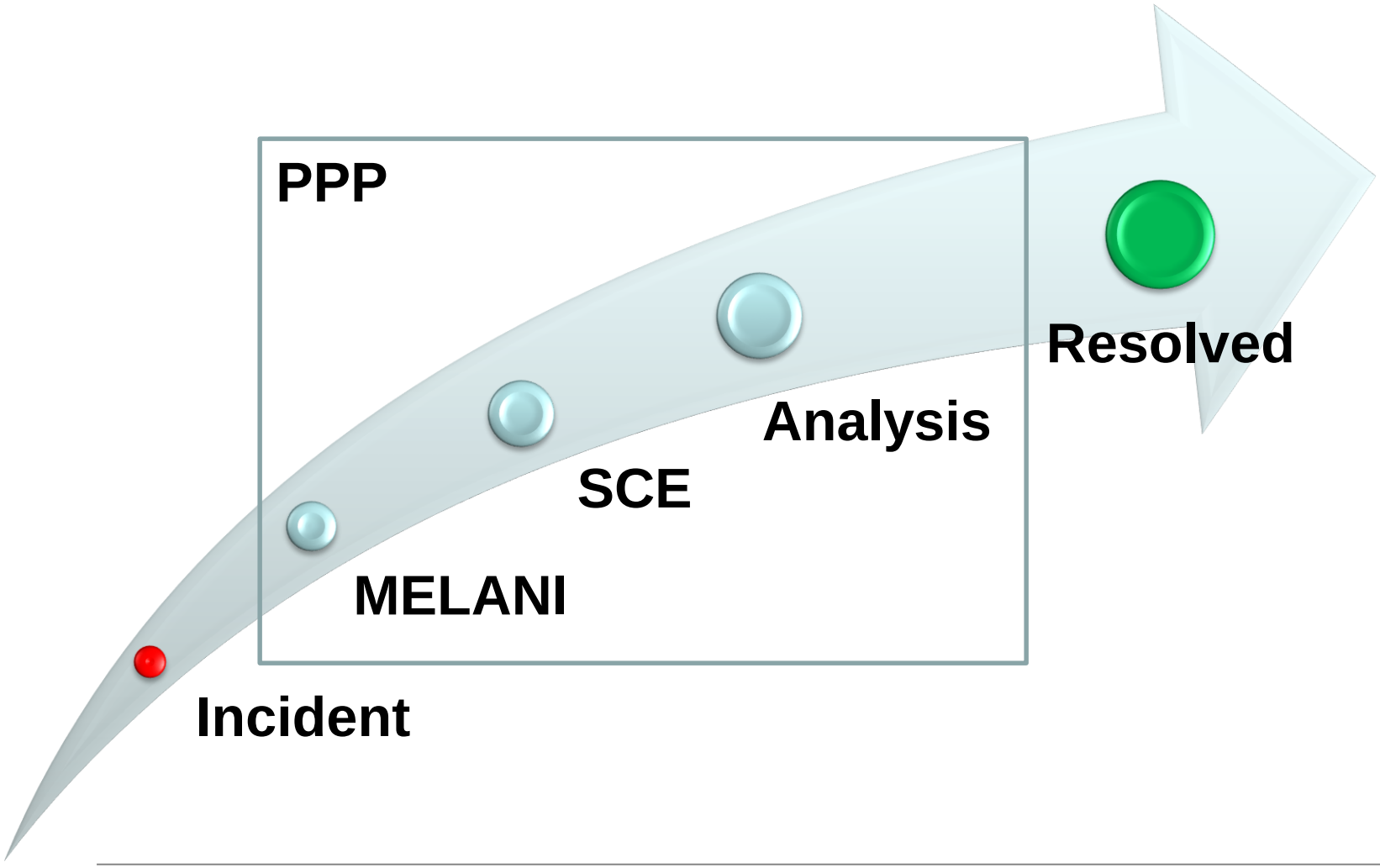
M5: Incident Handling	• Follow up and resolution of all relevant incidents • MELANI's PPP model: collection, identification, evaluation, analysis and made available to all the relevant actors
M12: Continuity MGMT	• Public-Private cooperation and continuity management in order to improve resilience and disruptions to cyber incidents • MELANI supports and strengthens the voluntary information exchange with CI operators in support of continuity and resilience based on individual self-help

The new mechanism



The SPOC MELANI will be strengthened.

Process from Incident to Resolution



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

Dr. Alain Gut, Director Public Sector, IBM Schweiz

Cybercrime und Cybersecurity -

The necessity of a Cyber Expert Pool for Switzerland

Scope: Security risk is increasing

Embracing New Technologies, Adopting New Business Models

Exploding and Interconnected Digital Universe

33% of all new business software spending will be Software as a Service

«Public» has to…

1. protect it's own infrastructure and services
2. Protect citizens, companies and – foremost – the critical infrastructures
3. Invest in this protection proactively

«Private» has to…

1. Understand future threats (F&E: centres and studies)
   a. Publish potential threats and respective measurements
2. Collaborate (internationally)
3. Collaborate with public security authorities, justice & police, data protection

Given the general need for security and the dynamics of ICT, collaboration of «public» and «private» is an ethical, mutual duty – e.g. in the field of information and knowledge exchange.

Do we have to add something new?

1. **Is there a need for support?**
   - Who's need is it? In which context? – 2012/13

2. **What would be a good solution?**
   - Initial concept(s) – 2012/13
   - Test: «Rheingold» – 2013
   - Conclusion: The solution through a private Association and a collaboration contract will work best

3. **Formalising Collaboration**
   - Founding the private association – 2014, done
   - Negotiating the contract – 2014, ongoing

E.g.: Why did we join?

X-Force – the Base of the IBM Security Frameworks

The mission of X-Force is to:

- Monitor and evaluate the rapidly changing threat landscape
- Research new attack techniques and develop protection for tomorrow's security challenges
- Educate our customers and the general public

Collaborative IBM teams monitor and analyze the world

Coverage

20,000+ devices under contract

3,700+ managed clients worldwide

15B+ events managed per day

133 monitored countries (MSS)

1,000+ security related patents

IBM Research

Depth

17B analyzed web pages & images

40M spam & phishing attacks

76K documented vulnerabilities

Billions of intrusion attempts daily

Millions of unique malware samples

IBM X-Force Report 1Q 2014

More than **half a billion records**
of personally identifiable information (PII) were leaked in 2013

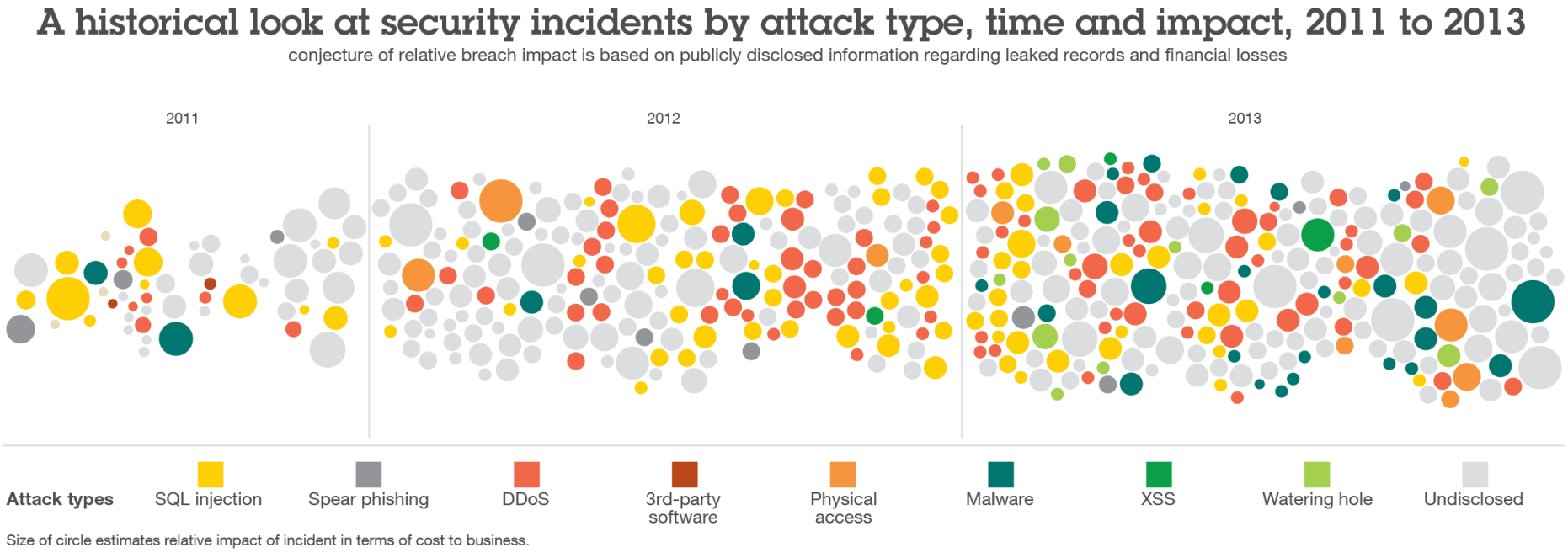
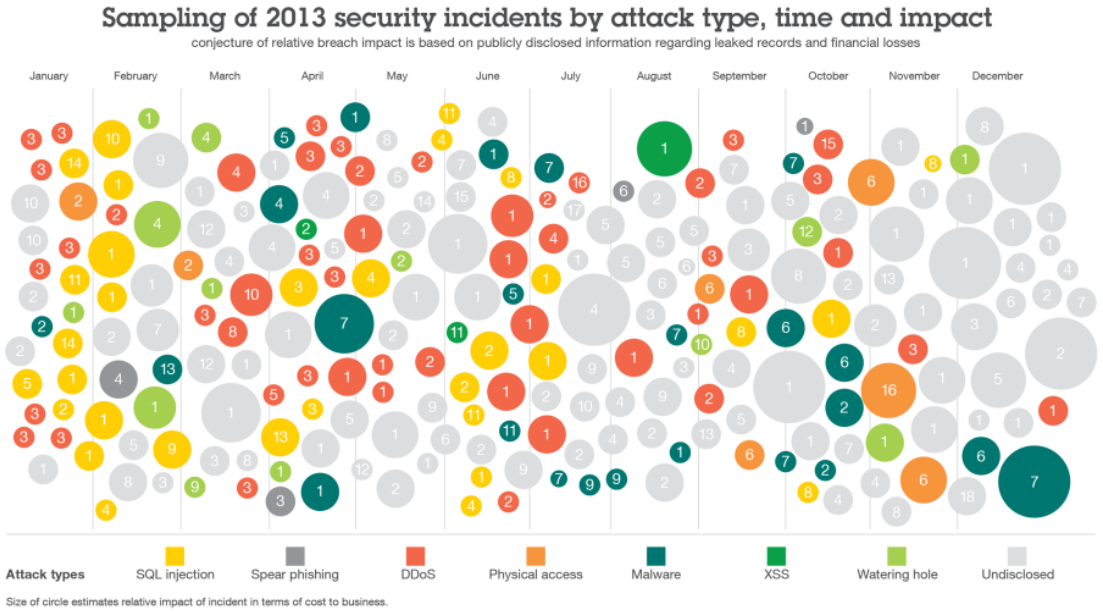


Figure 1. A historical look at security incidents by attack type, time and impact, 2011 to 2013

Source: IBM X-Force® Research and Development

Government is one of the main targets



Most-commonly attacked industries

28%	Computer Services (1)
15%	Government (2)
12%	Financial Markets (3)
9%	Media & Entertainment (4)
7%	Education (5)
5%	Healthcare (6), Retail (7), Telecommunications (8)
3%	Consumer Products (9)
2%	Non-Profit (10), Automotive (11), Energy & Utilities (12), Professional Services (13)
1%	Industrial Products (14), Travel & Transportation (15), Wholesale Distribution & Services (16)
<1%	Aerospace & Defense (17), Insurance (18)

Most-common attack types

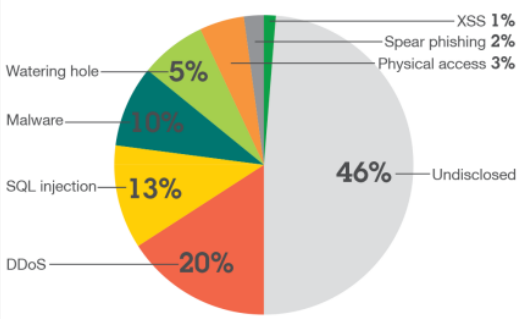


Figure 2a. Sampling of 2013 security incidents by attack type, time and impact

Source: IBM X-Force® Research and Development

Swiss Cyber Experts (SCE)

The associations charter states – in German:

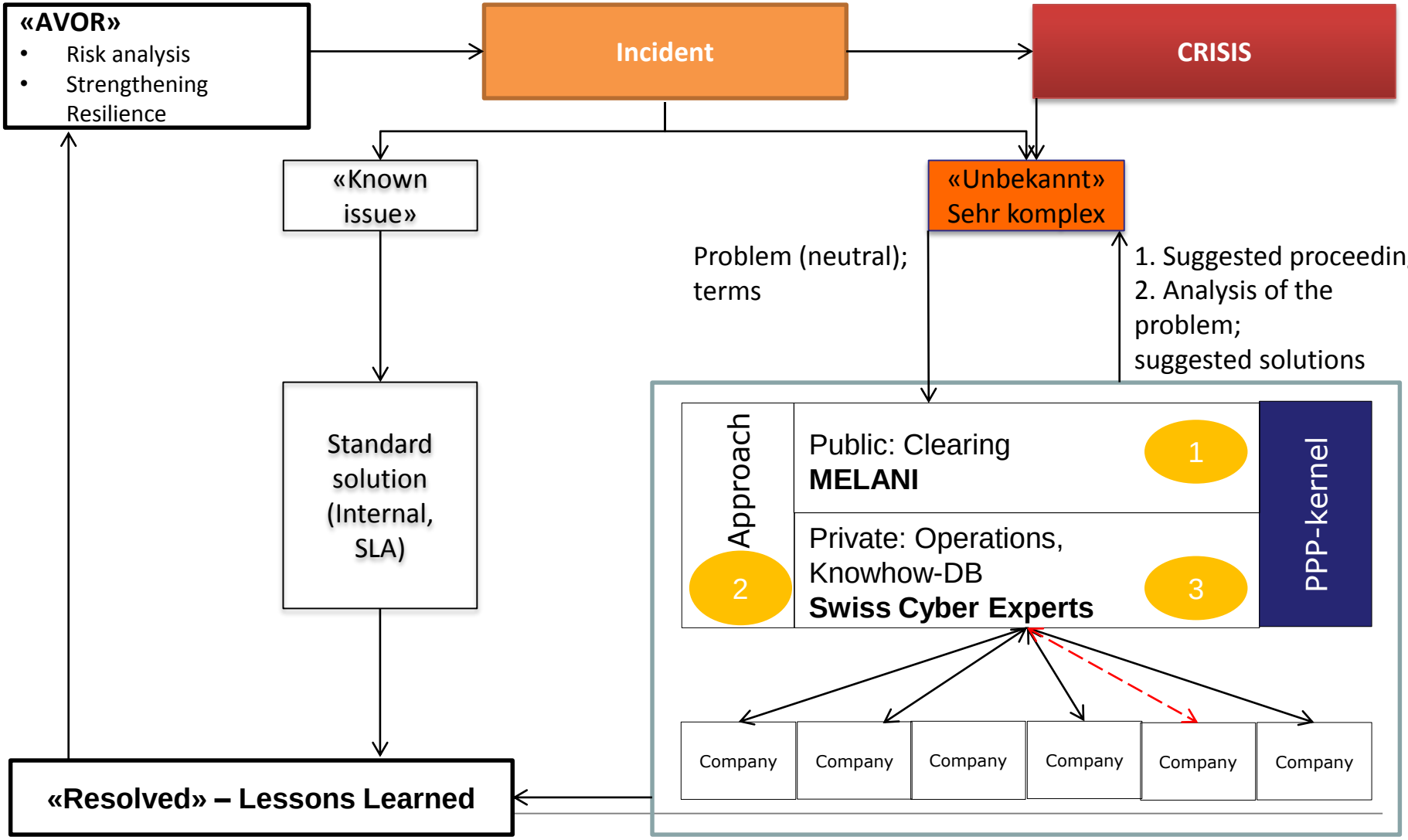
«Es geht darum, ein Mittel zu schaffen, **im Falle eines schweren Incidents auf effiziente Art auf Expertenwissen aus der ICT-Industrie zugreifen zu können**. Es ist das Anliegen der Vereinsmitglieder, schwere Cyber-Incidents schnell zu erkennen und so zu analysieren, dass sie von den vertraglich verpflichteten Firmen effektiv behoben werden können.

Der Verein steht Schweizer (Tochter-) Firmen offen, die Experten zum Pool beisteuern und damit substanzielle Beiträge zur Beurteilung schwerer Cyber-Incidents leisten **können**.»

- In the case of a grave incident…
- private ICT-experts shall be accessible efficiently…
- to analyse the problem.

- The association is open to all companies that can contribute genuine expertise.

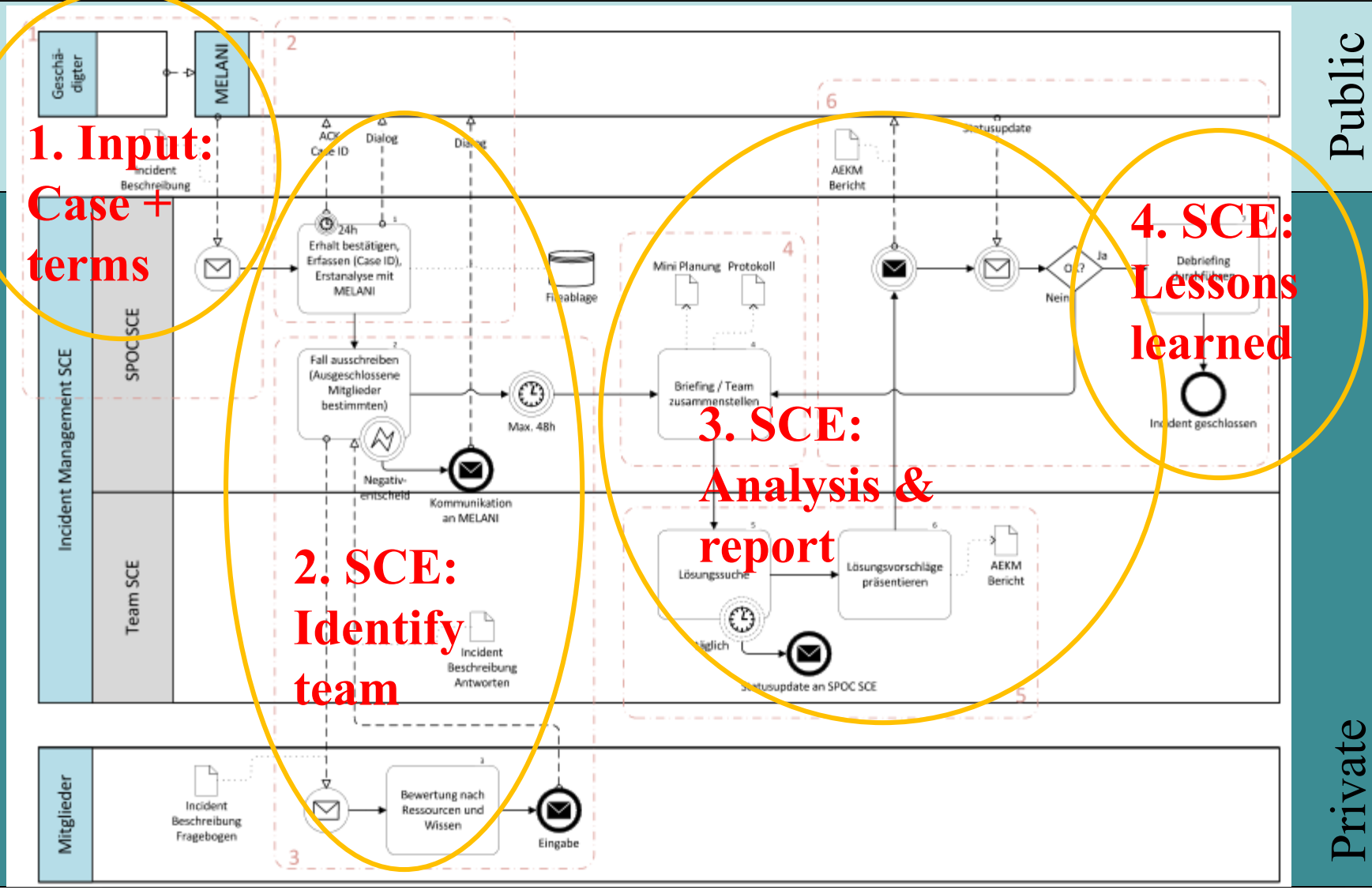
The process in detail



SCE-Processes

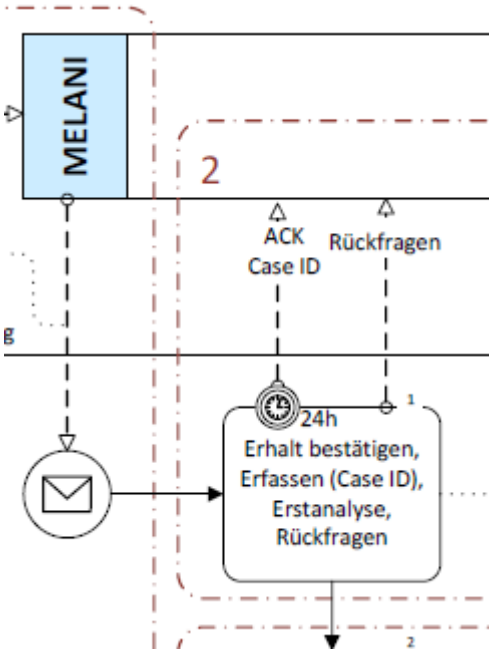
Public

Private



Terms:
The victims information and decisions

1. **Mission**
   a. Description of the problem
   b. Urgency
   c. Desired processes (involvement of victim)
   d. Biggest risks
   e. Victims means that did not help



2. **Confidentiality**
   a. Secret / confidential / non critical
   b. Foreign experts allowed?
   c. Excluded companies
   d. Analysis on site required?
   e. Victim not to be disclosed by MELANI
   f. SCE-internal debriefing (for all members) allowed?

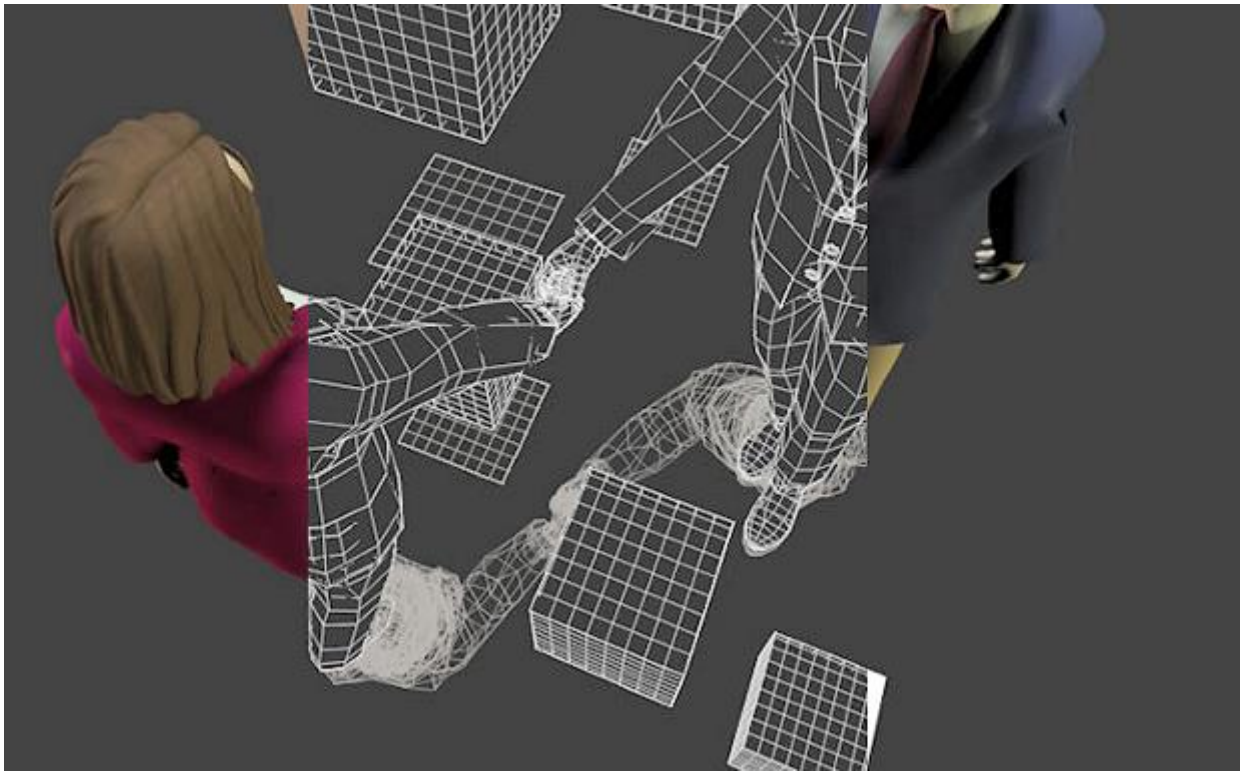
SCE-Members

- **IBM Schweiz (President)**
- netnea.com (Vice-President)
- T-Systems Schweiz (Vice-President)

- e3 AG
- idQuantique
- InIT, ZHAW
- Koramis GmbH
- Kudelski Security
- PWC Schweiz
- RISIS, BFH
- RUAG
- Swiss Infosec

Status as per October 2014. Some members chose confidentiality.

Thank you for your attention



Dr. Alain Gut
Director Public Sector, IBM Switzerland
President Swiss Cyber Experts
Mobile: +41 79 235 0774 – alain.gut@ch.ibm.com