Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesamt für Energie BFE
Office fédéral de l'énergie OFEN
Ufficio federale dell'energia UFE
Uffizi federal d'energia UFE

DIALOGPLATTFORM DIGITALISIERUNG CYBER SECURITY UND CYBER RESILIENZ

BUNDESAMT FÜR ENERGIE ▪ DIGITAL INNOVATION OFFICE ▪ 22. SEPTEMBER 2021

AGENDA

09:15 Begrüssung Teilnehmende Dialogplattfom	M. Galus (BFE)
09:20 Future of Cyber Security in the Electricity Sector *Network Code on Cyber Security in EU.*	M. Barroso Gomes (ACER)
09:50 Cyber Maturität im Schweizer Energiesektor Ergebnisse und Perspektiven	R. Häni (Deloitte)
10:30 Pause	
10:45 Massnahmen und Nächste Schritte	S. Henry (BFE)
11:00 Reflektionen in der Dialogplatform	Alle, Moderator M. Galus (BFE)
11:45 Ende Veranstaltung	

ACER

European Union Agency for the Cooperation of Energy Regulators

Framework guideline on sector-specific rules for cybersecurity aspects of cross-border electricity flows

Maria Barroso Gomes

Dr. Ing Manuel Sánchez-Jiménez

Øyvind Anders Arntzen Toftegaard

22 September 2021

Presentation to the Federal Department of the Environment, Transport, Energy and Communications

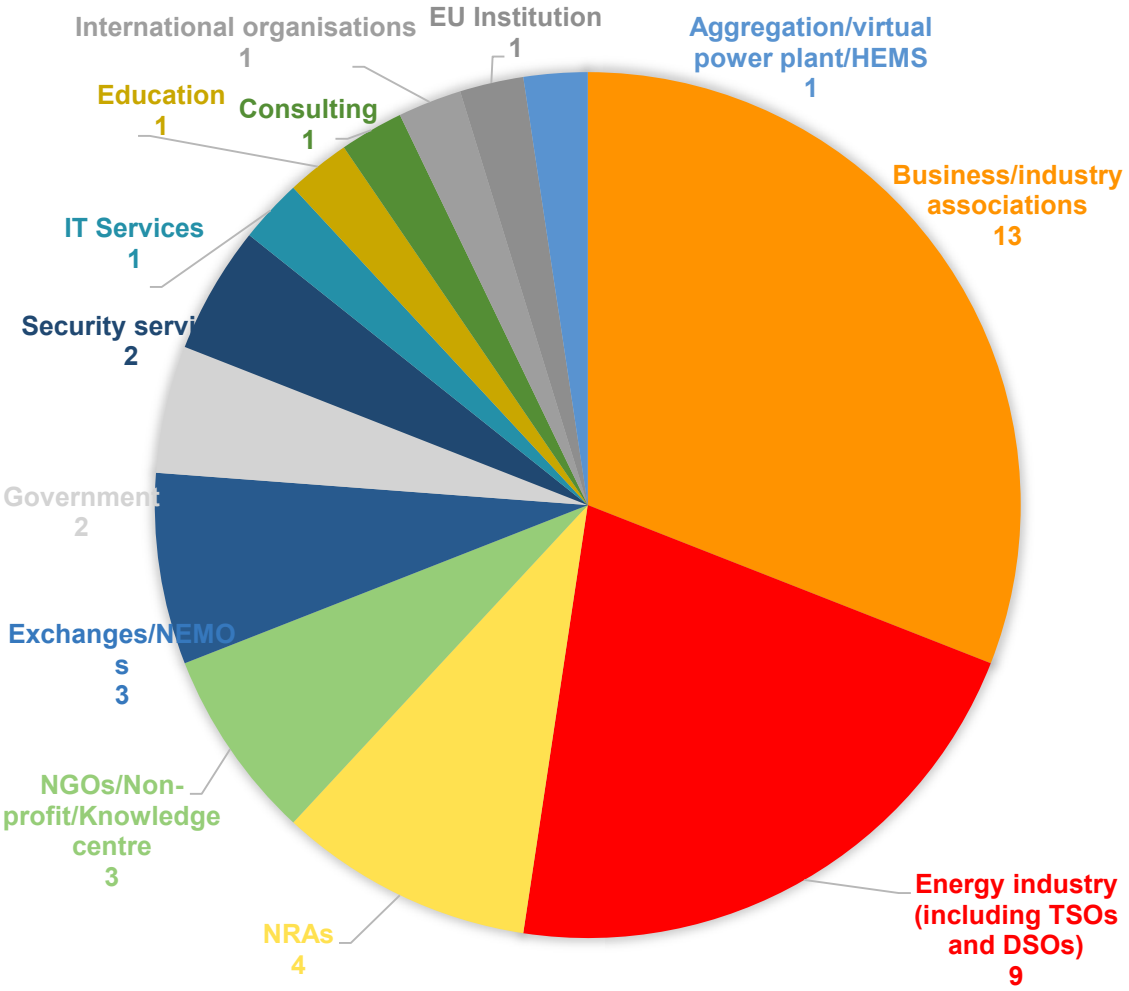
Swiss Federal Office of Energy SFOE

ACER
European Union Agency for the Cooperation of Energy Regulators

Timeline recap

- **30 Apr 2021:** FG proposal on public consultation
- **25 June 2021:** Revised draft FG shared with AEWG
- **29 June 2021:** Deadline for comments on the public consultation
- **7 July 2021:** Revised draft FG shared with AEWG for their endorsement
- **13 July 2021:** AEWG endorsed the revised draft FG
- **15 July 2021:** Revised FG shared with BoR for their opinion
- **22 July 2021:** Favourable opinion of BoR
- **22 July 2021:** FG sent by ACER to the Commission
- **23 July 2021:** EU Commission sent the request to submit a proposal for a CSNC to ENTSO-E

Results of the public consultation



- Respondents in general welcome the draft FG
- 88% believe the draft FG contributes to further protecting cross border electricity flows
- 85%, consider that FG covers sufficiently the real-time requirements of energy infrastructure components, the risk of cascading effects and the mix of legacy and state-of-the-art technology
- 65% believe the draft FG still have gaps concerning the cybersecurity of cross-border electricity flows, which the FG should address

Recap on FG content

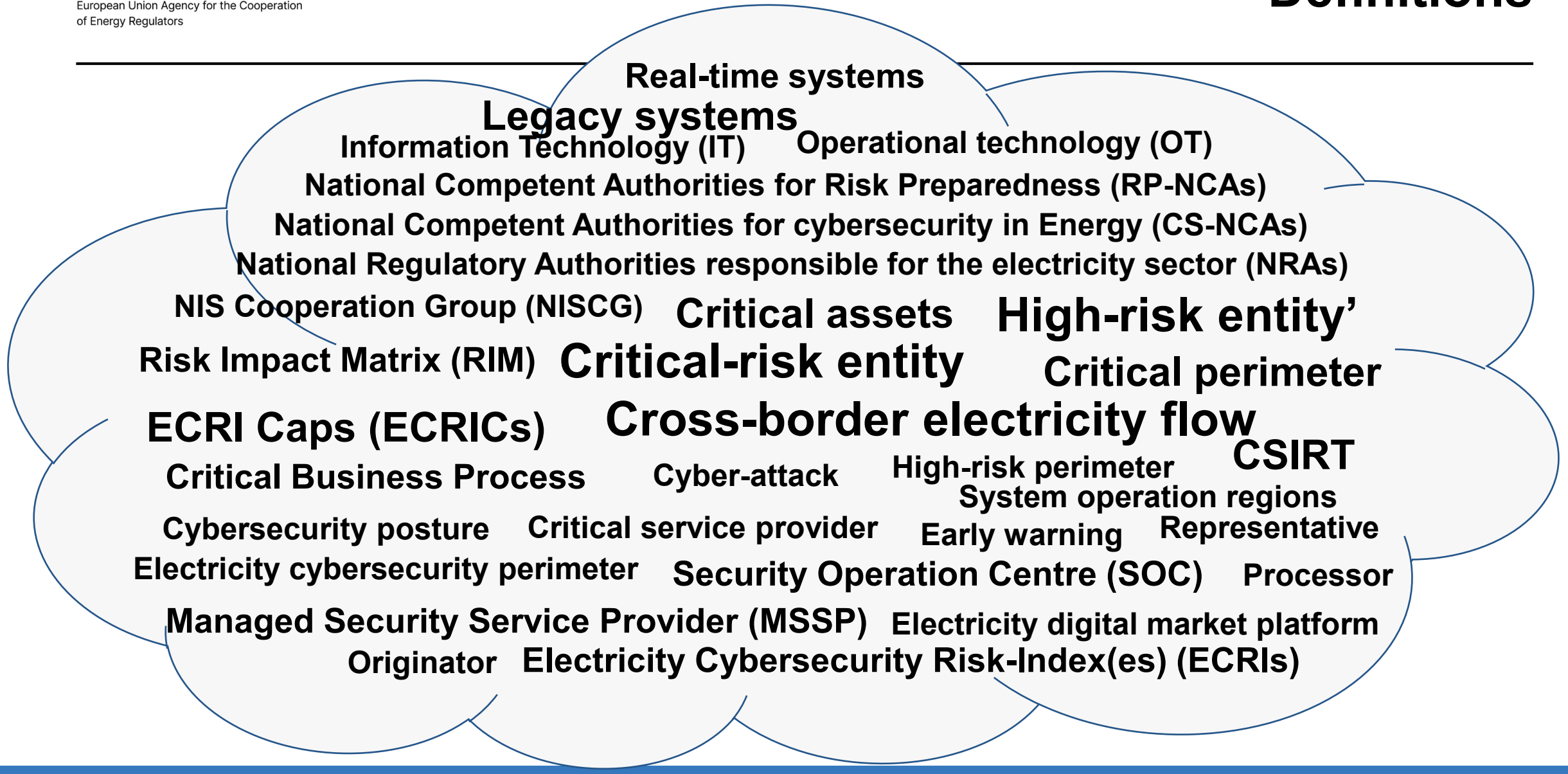
1. **General Provisions**: scope, definitions, applicability and transitional measures
2. **Cybersecurity Electricity Governance**: general principles
3. **Cybersecurity Risk Assessment**: integrated approach, its governance and transitional methodology

4. **Common Electricity Cybersecurity Framework**: governance for the definition of minimum and advanced requirement, and supply chain
5. **Essential information flows, Incident and Crisis Management**
6. **Electricity Cybersecurity exercise framework**

7. **Protection of information exchanged in this network code**
8. **Monitoring, benchmarking and reporting**
9. **New systems, process and procedures**

ACER
European Union Agency for the Cooperation of Energy Regulators

Definitions



ACER
European Union Agency for the Cooperation of Energy Regulators

Applicability of the CSNC

#	Table 1. Entity definition
1	Electricity undertakings as defined in Article 2(57) of the Electricity Market Directive
2	NEMOs as defined in Article 2(7) and (8) of Electricity Market Regulation
3	Electricity digital market platforms as defined in this Framework Guideline
4	Critical service providers as defined in this Framework Guideline
5	Regional Coordination Centres (RCCs) established pursuant to Article 35 of the Electricity Market Regulation
6	ENTSO-E, the EU DSO entity, ACER and NRAs
7	RP-NCAs, SOCs, CS-NCAs and CSIRTs and ENISA

The **network code must provide for the possibility of applying** it to small and micro enterprises as well as any additional stakeholders at the initiative of:

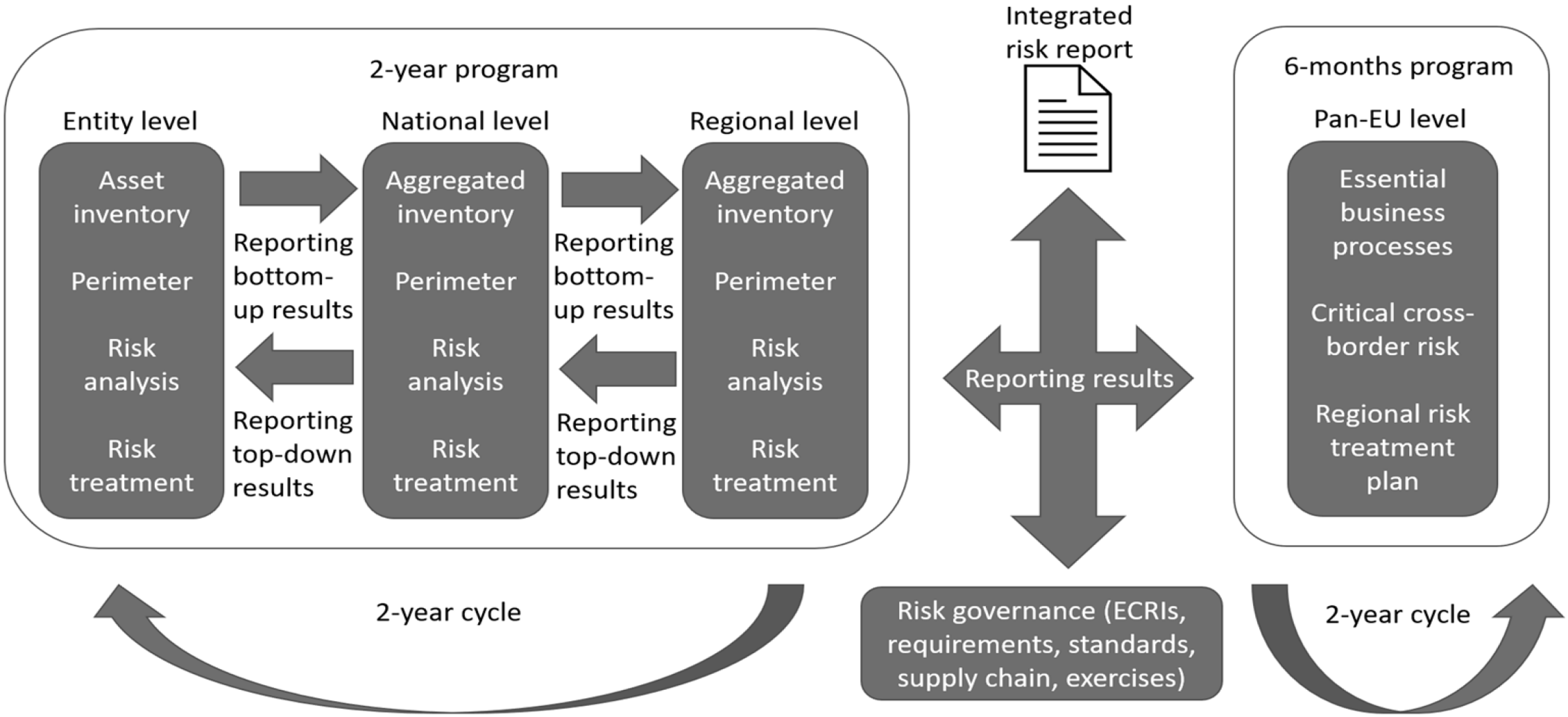
i. any entity listed in Table 1, after consulting and having obtained an opinion from the competent NRA(s) and the CS-NCAs;

ii. the CS-NCA jointly with the respective NRA of the concerned Member State; or

iii. the European Commission, following an ACER opinion, after consulting and having obtained an opinion from the competent NRA(s) and the CS-NCAs.

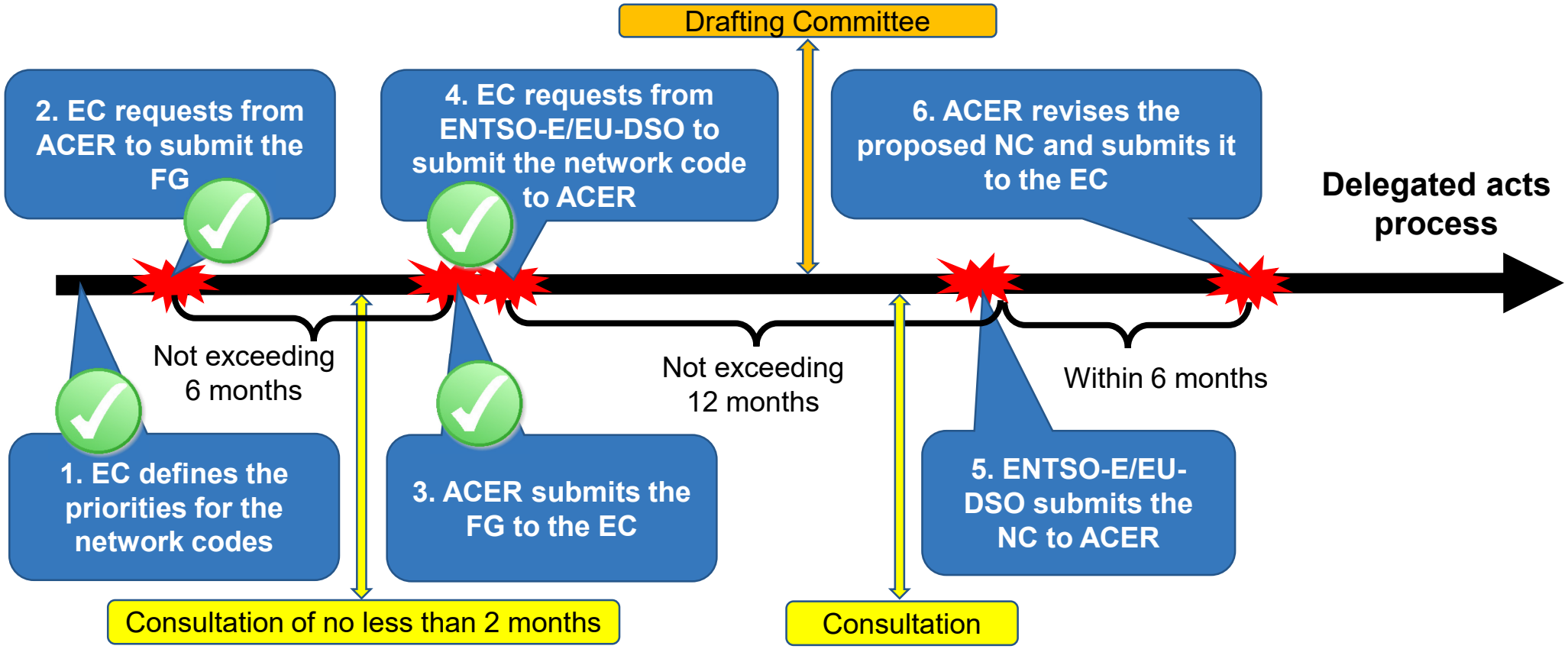
ACER
European Union Agency for the Cooperation of Energy Regulators

Integrated top-down and bottom-up approach



Time schedule (completed and next steps)

- **General timeline as set out in Article 59 of REGULATION (EU) 2019/943**



Øyvind Anders Arntzen Toftegaard

Dr. Ing Manuel Sánchez-Jiménez
Manuel.SANCHEZJIMENEZ@acer.europa.eu

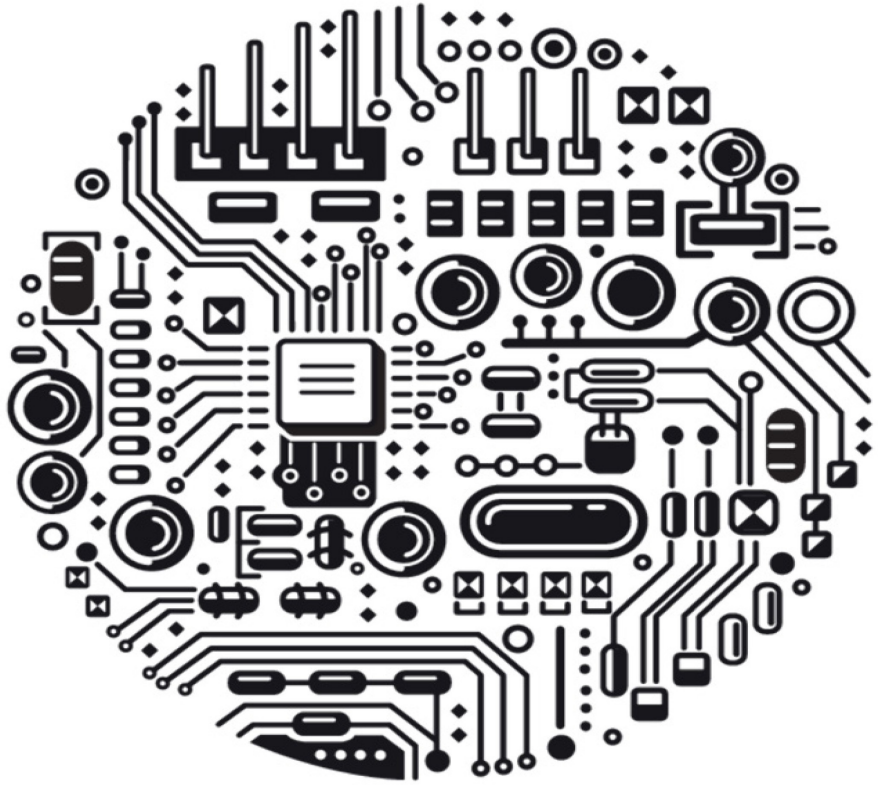
Maria Barroso Gomes
Maria.BARROSOGOMES@acer.europa.eu

DISCUSSION & QUESTIONS

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesamt für Energie BFE
Office fédéral de l'énergie OFEN
Ufficio federale dell'energia UFE
Uffizi federal d'energia UFE

Deloitte.



CYBER-SICHERHEIT UND RESILIENZ FÜR DIE SCHWEIZER STROMVERSORGUNG

INHALTSVERZEICHNIS

1 Einleitung

2 Ausgangslage

3 Internationaler Vergleich

4 Aktueller Stand betreffend Cyber-Maturität

5 Vorschläge zur Verbesserung

6 Fazit

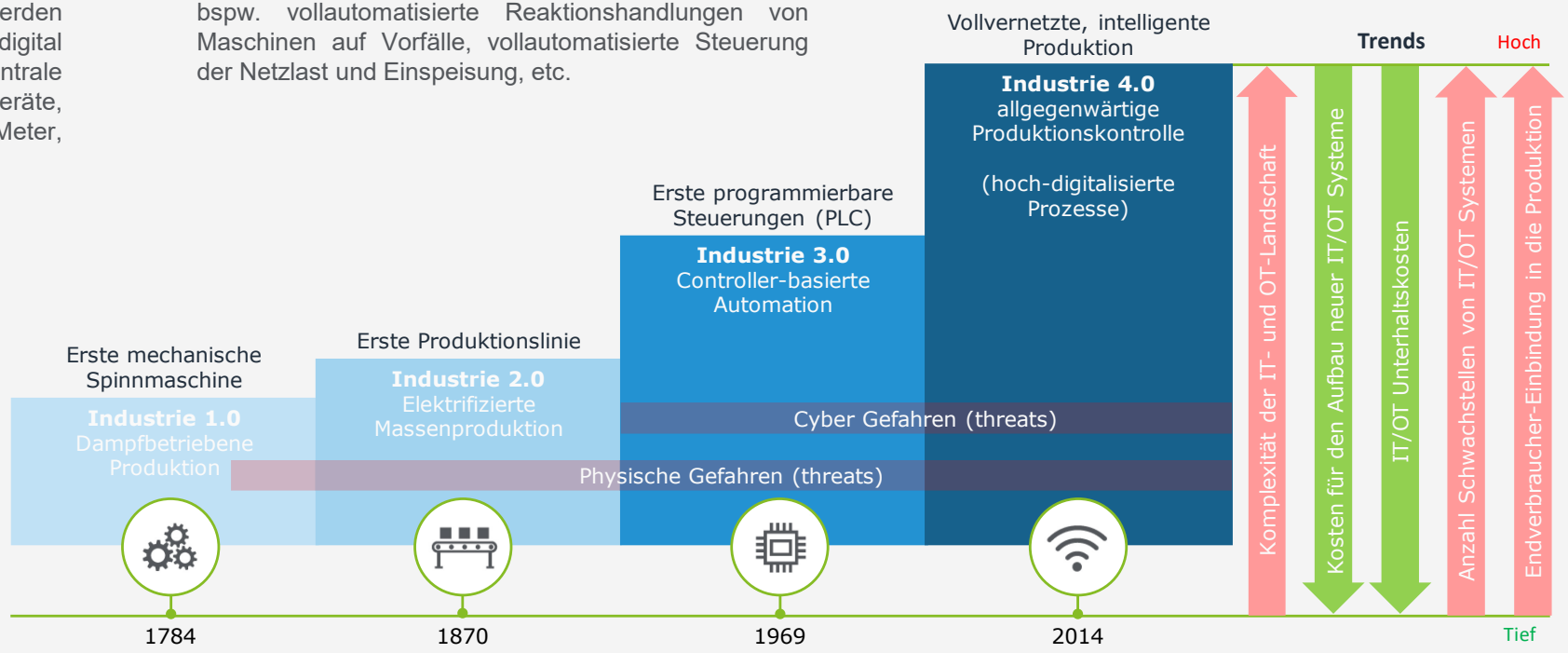
1. **EINLEITUNG** | DIGITALISIERUNG IM STROMSEKTOR – EINE VIELZAHL NEUER MÖGLICHKEITEN UND RISIKEN

Informations- und Kommunikationstechnologien (IKT) werden zu einem immer integraleren Bestandteil der Wertschöpfungskette der elektrischen Energieversorgung. Eine zunehmende Digitalisierung ermöglicht viele positive Entwicklungen und fördert neue wirtschaftliche Aktivitäten, bringt jedoch auch neue Risiken und Gefahren – insbesondere aus Sicht der Informationssicherheit und Resilienz.

«Internet of Things» (IoT) und «5G»
Viele Komponenten entlang der kompletten Wertschöpfungskette vom Produzenten bis hin zum Endverbraucher werden zunehmend intelligenter und digital miteinander vernetzt – bspw. dezentrale Stromerzeugungs- und Speichergeräte, aktive Netzkomponenten, Smart Meter, Haushaltsgeräte, Elektroautos, etc.

«Big Data» und «Cloud»
Eine zunehmende Nutzung von Cloud-Dienstleistungen und damit verbunden eine grössere Abhängigkeit von Drittparteien. Auch begünstigen Cloud-Technologien bspw. neue Netzsteuerungsmöglichkeiten, sowie eine vereinfachte Integration und Zusammenarbeit mit kleineren Produzenten, Netz- und Messtellen-betreibern, etc.

«Artificial Intelligence» (AI)
Eine zunehmende Nutzung künstlicher Intelligenz und vollautomatisierter Algorithmen innerhalb des Sektors – bspw. vollautomatisierte Reaktionshandlungen von Maschinen auf Vorfälle, vollautomatisierte Steuerung der Netzlast und Einspeisung, etc.



2. **AUSGANGSLAGE** | EINE STARK FRAGMENTIERTE, HISTORISCH GEWACHSENE REGULATIONSLANDSCHAFT

Eine Auswahl derzeit bestehender Vorgaben	Was wird aus Sicht Cyber und Resilienz derzeit geregelt?
Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken 2018-2022 (NCS)	Die Strategie soll dazu beitragen, dass die Schweiz bei der Nutzung der Chancen der Digitalisierung angemessen vor Cyber-Risiken geschützt und ihnen gegenüber resilient ist
Nationale Strategie zum Schutz Kritischer Infrastrukturen (SKI)	Massnahmen mittels welcher die Versorgungssicherheit allgemein erhalten und noch verbessert werden soll — insbesondere auch für elektrische Landesversorgung
Landesversorgungsgesetz (LVG)	Subsidiär präventive Massnahmen hinsichtlich der Erarbeitung von Cyber-Standards für die Wirtschaft — insbesondere für die Stromversorgung
Energiegesetz (EnG)	Art. 7 EnG hält Leitlinien für eine sichere Energieversorgung fest — insbesondere auch der Schutz kritischer Infrastrukturen einschliesslich der zugehörigen IKT
Stromversorgungsgesetz (StromVG)	Art. 8 StromVG verpflichtet Netzbetreiber ein «sicheres, leistungsfähiges und effizientes Netz» zu gewährleisten — d.h. es impliziert Massnahmen zur IKT-Sicherheit, konkretisiert diese aber nicht
Stromversorgungsverordnung (StromVV)	Art. 8a und in Art. 8b StromVV verweisen auf die Verpflichtung eines Branchenstandards im Bereich der Datensicherheit betreffend intelligente Messsysteme
Freiwillige Mindeststandards für Cyber-Sicherheit • «IKT Minimalstandard» des BWL • «Handbuch Grundschutz für Operational Technology» des Branchenverbandes (VSE)	Empfehlungen und mögliche Leitfäden zur Verbesserung der allgemeinen IKT-Resilienz – primär entlang einer adaptierten Version des NIST Cybersecurity Frameworks (CSF v1.1) und ebenfalls im Einklang mit weiteren, international anerkannten Standards

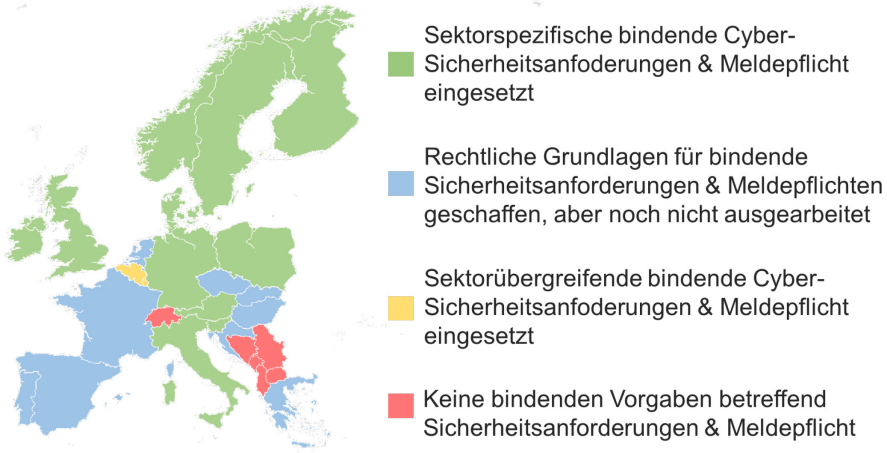
Fazit: Cyber-Sicherheit und Resilienz ist Stand heute weder einheitlich noch flächendeckend für alle relevanten Akteure innerhalb des Schweizer Stromsektors geregelt – weiterführende, verpflichtende Vorgaben und Mindestanforderungen sind innerhalb des Sektors bisher ausstehend

3. INTERNATIONALER VERGLEICH | ÄHNLICHE STOSSRICHTUNGEN, JEDOCH UNTERSCHIEDLICHE FORMEN UND STAND DER UMSETZUNG

Mittels Quervergleich mit anderen Ländern betreffend reguArialrische Situation für Cyber-Sicherheit und Resilienz im jeweils lokalen Stromsektor wurde erkannt, dass die grundsätzliche Stossrichtung der Schweizer NCS 2018-2022 auch in anderen Ländern auffindbar ist.

Insbesondere die Entwicklungen innerhalb der EU sind relevant, da eine sehr starke technische und organisatorische Vernetzung der Stromsysteme der Schweiz und der EU-Mitgliedstaaten besteht, vor allem mit den unmittelbaren Nachbarländern. Entsprechend gross sind die wechselseitigen Abhängigkeiten voneinander.

Bindende EU-Vorgaben	Kurze Beschreibung
EU Richtlinie für die Sicherheit von Netz- und Informationssystemen **(NIS-Richtlinie)** *NIS1 trat 2016 in Kraft und wird bereits mit Hochdruck überarbeitet und weiterentwickelt*	Das Ziel der NIS-Richtlinie ist es ein gleichmässig hohes Sicherheitsniveau von Netz- und Informationssystemen in der gesamten EU zu erreichen *Für Details und einen Quervergleich mit dem Umsetzungsstand in der Schweiz siehe Slide 6*
Energiespezifischer «Cybersecurity Network Code» *Erster Entwurf wird Mitte 2021 erwartetet*	Wird von European Network of Transmission System Operators for Electricity (ENTSO-E) und EU Distribution System Operator Entity (EUDE) erarbeitet und wird technische Anforderungen an Netzbetreiber und -anschlussnehmer konkretisieren



Quelle: Bird & Bird (2020), Developments on NIS Directive in EU Member States

Fazit: Die in der NCS 2018-2022 festgehaltenen Stossrichtungen des Bundes sind grösstenteils mit den Massnahmen der ersten NIS-Richtlinie der EU kompatibel**.** Der aktuelle Vorsprung der EU Staaten im Bereich der Cyber Sicherheit und Resilienz ist derzeit jedoch beachtlich. Viele der für die Schweiz aktuell diskutierten Massnahmen sind aufgrund der NIS-Richtlinie andernorts in der EU bereits in der Praxis umgesetzt, operativ und längst etabliert.

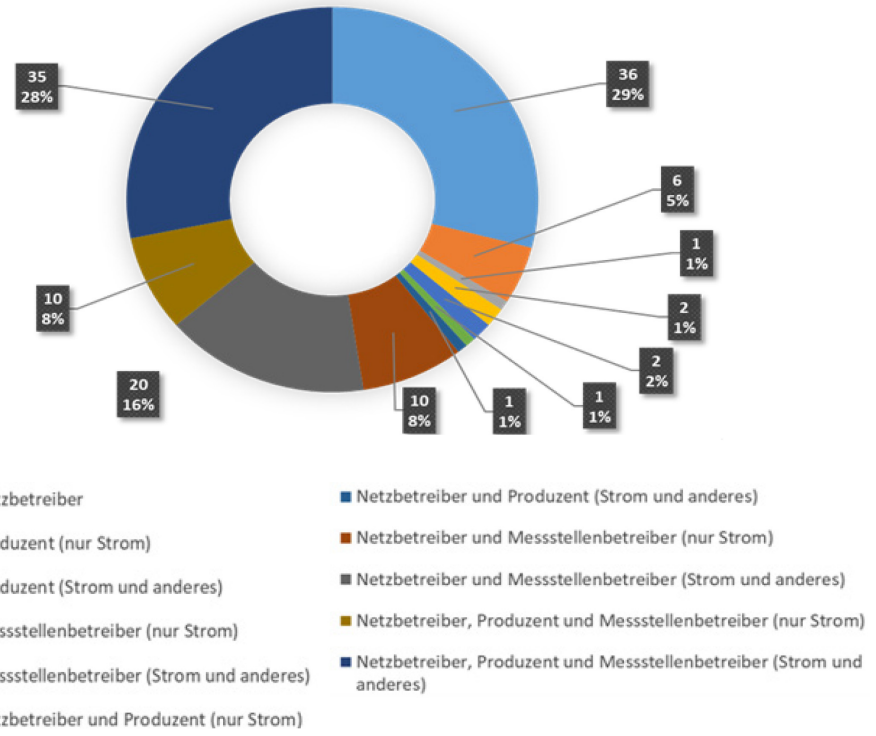
3. INTERNATIONALER VERGLEICH | ÄHNLICHE STOSSRICHTUNGEN, JEDOCH UNTERSCHIEDLICHE FORMEN UND STAND DER UMSETZUNG

Verpflichtungen gemäss EU NIS1			Mapping zu CH NCS 2018-2020	Umsetzungsstand in der Schweiz	Identifizierter Handlungsbedarf für den Schweizer Stromsektor
# 1	Nationale Strategie		**Verabschiedung der NCS 2018-2022**		(Keiner)
# 2	EU-Kooperationsgruppe		Nicht direkt anwendbar, da kein EU-Mitgliedsstaat und daher nicht Mitglied der Gruppe.		
# 3	Netzwerk von Computer-Notfallteams		Nicht direkt anwendbar, da kein EU-Mitgliedsstaat, aber gewisse Relevanz für GovCERT.ch (offizielles Computer Emergency Response Team der Schweiz)		
# 4	Sicherheits-anforderungen und Meldepflichten	Sicherheits-anforderungen	**NCS Massnahme 8:** Evaluierung und Einführung von Minimalstandards		Institutionalisierte *Rahmenbedingungen* betreffend Cyber-Sicherheit und Resilienz im Schweizer Stromsektor und damit verbunden, die Schaffung geeigneter und verhältnismässiger, technischer und organisatorischer Sicherheitsanforderungen für Cyber-Sicherheit und Resilienz innerhalb des Stromsektors Schweiz.
		Meldepflicht	**NCS Massnahme 9:** Prüfung einer Meldepflicht für Cyber-Vorfälle und Entscheid über Einführung		Das institutionalisierte *Meldewesen* betreffend laufende Cyber-Attacken innerhalb des Stromsektors Schweiz, inklusive der Einführung einer Meldepflicht.
		Überprüfung	**Impliziert durch NCS Massnahme 8**		Die institutionalisierte *Überprüfung* der getreuen Umsetzung bestehender Cyber-Regulierungen durch die Marktteilnehmer des Stromsektors Schweiz.
# 5	Ernennung von:	Nationale zuständige Behörden	**Allgemeine Bestimmungen der NCS und NCS Umsetzungsplan**		Die Festlegung von *Verantwortlichkeiten* (Institutionalisierung) für Cyber-Rahmenbedingungen, -Überprüfung, -Wissensaustausch und -Meldewesen im Stromsektor.
		Zentrale Anlaufstelle	**Schaffung NCSC im Rahmen der NCS**		(Keiner)
		Nationales Computer Emergency Response Team	**NCS Massnahme 4:** Ausbau der Fähigkeiten zur Beurteilung und Darstellung der Cyber-Bedrohungslage		Der institutionalisierte, laufende *Wissensaustausch* betreffend aktuelle Cyber-Gefahren (Threat Intelligence) innerhalb des Schweizer Stromsektors, sowie auf internationaler Ebene.

4. AKTUELLER STAND BETREFFEND CYBER-MATURITÄT | IM SCHNITT TIEFE WERTE FÜR UNTERNEHMEN DES SCHWEIZER STROMSEKTORS

Damit allenfalls die richtigen, künftigen Massnahmen für die Schweiz abgeleitet werden können, wurde daher erstmalig die aktuelle Lage betreffend Cyber-Maturität der relevanten Akteure innerhalb der Schweizer Stromversorgung erhoben. Dies erfolgte anhand des seit 2018 durch das Bundesamt für Wirtschaftliche Landesversorgung (BWL) und den Branchenverband Schweizer Elektrizitätswirtschaft (VSE) etablierten «IKT Minimalstandards» und wurde über eine elektronische Umfrage (E-Survey) abgefragt.

Unternehmenstyp	Repräsentation
113 Netzbetreiber	Gemäss Angaben der ElCom, rund 18% der Gesamtmenge aller existierenden Netzbetreiber der Schweiz im Jahr 2019
54 Produzenten	Etwa 50% aller grösseren Schweizer Stromproduzenten, welche durch das BFE für eine Teilnahme an der Umfrage angefragt wurden
79 Messstellenbetreiber	Die teilnehmenden Messtellenbetreiber decken gemeinsam ungefähr 40% aller im Jahr 2019 existierenden Messpunkte der Schweiz ab



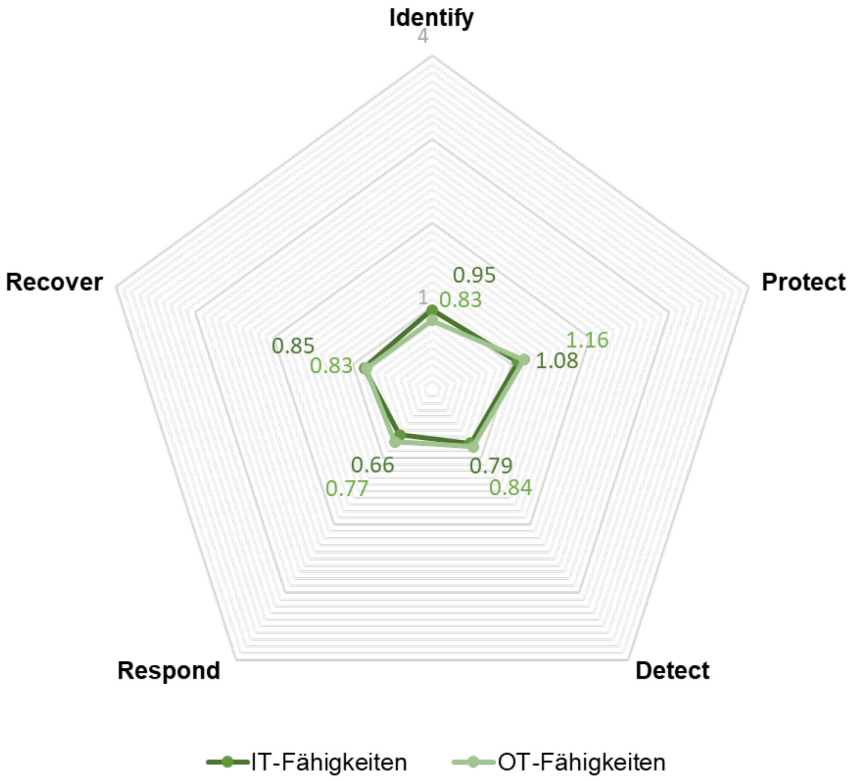
Insgesamt wurden etwa 750 Unternehmen um Mithilfe gebeten. Davon beteiligten sich 124 Unternehmen, welche über die verschiedenen Bereiche der Wertschöpfungskette innerhalb des Schweizer Stromsektors tätig sind (vertikal integrierte Unternehmen). Die Mehrheit der in der Umfrage vertretenen Rollen am Markt waren 113 Netzbetreiber gefolgt von 79 Messstellenbetreibern und 54 Produzenten (eine Unternehmung kann zeitgleich mehrere Rollen am Markt wahrnehmen).

4. AKTUELLER STAND BETREFFEND CYBER-MATURITÄT | IM SCHNITT TIEFE WERTE FÜR UNTERNEHMEN DES SCHWEIZER STROMSEKTORS

Die Umfrageteilnehmer wurden gebeten, die eigene Maturität entlang dem IKT Minimalstandard selbst einzuschätzen (siehe auch Anhang 1).

Die E-Survey führte zu den folgenden Schlüssel-Erkenntnissen:

- Cyber-Sicherheit wird oftmals noch immer als eine Nebentätigkeit mit geringer Management-Priorität innerhalb der Unternehmen angesehen
- Das Vorhandensein einer klar ausformulierten IT-/OT-Strategie korreliert stark positiv mit den entsprechenden Maturitätswerten der Unternehmen
- Die Verantwortlichkeiten und Prozesse für Cyber-Sicherheit und Resilienz ist bei vielen Unternehmen noch nicht institutionalisiert
- Cyber-Risiken werden offenbar meist auf einer ad-hoc und/oder reaktiven Basis verwaltet
- Risikomanagementprozesse und organisatorische Vorgaben betreffend IKT-Sicherheit scheinen oftmals nicht formalisiert
- Die Funktionen «Erkennen» und «Reagieren» verzeichnen im Schnitt die tiefsten Maturitätswerte – dies ist bedauerlich, da ausgerechnet diese Fähigkeiten besonders wichtig sind, um auf grössere Cyber-Vorfälle zeitnah und adäquat reagieren zu können
- Eine grosse Mehrheit der Umfrageteilnehmer (69%) befürwortet eine Meldepflicht von Cyber-Sicherheitsvorfällen

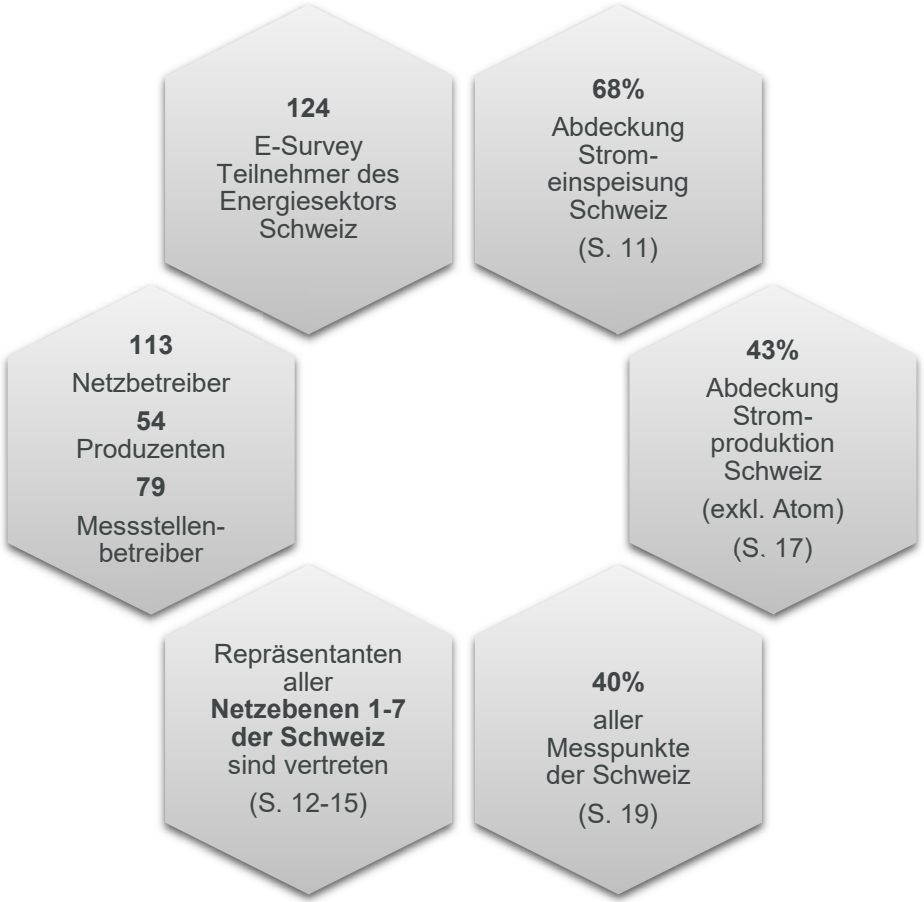


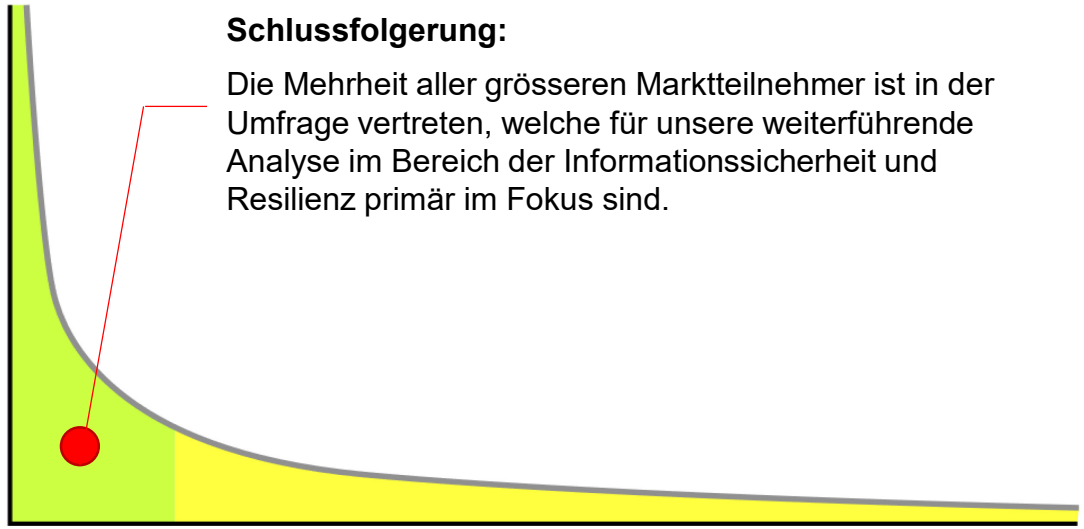
Fazit: Die Auswertung der E-Survey bezüglich IT-/OT-Sicherheits-Maturität der Schweizer Strommarktteilnehmer zeigt deutlich, dass die Akteure bisher noch nicht selbstständig und auf freiwilliger Basis alle notwendigen Massnahmen getroffen haben, um den steigenden Cyber-Risiken adäquat entgegenzuwirken – die Betriebe sind demnach der eigenen Branchenrichtlinie nicht nachgekommen und noch weit entfernt von dem eigens gesetzten Ziel eines durchschnittlichen Maturitätswerts von «2.6» über alle Bereiche.

4. AKTUELLER STAND BETREFFEND CYBER-MATURITÄT | E-SURVEY

ALLGEMEINER TEIL

Zusammenfassend konnte die Umfrage insgesamt eine repräsentative Teilnahme des Energiesektors Schweiz erzielen:



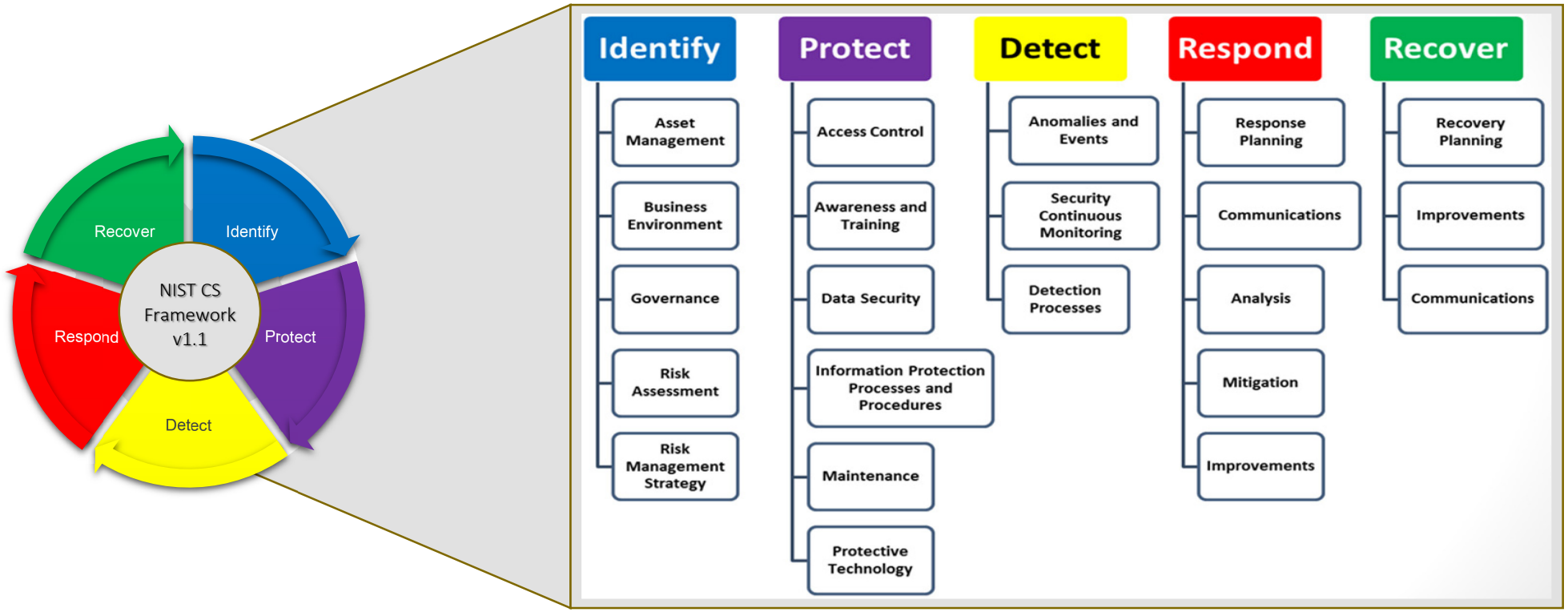


Schlussfolgerung:

Die Mehrheit aller grösseren Marktteilnehmer ist in der Umfrage vertreten, welche für unsere weiterführende Analyse im Bereich der Informationssicherheit und Resilienz primär im Fokus sind.

4. AKTUELLER STAND BETREFFEND CYBER-MATURITÄT | IKT MINIMALSTANDARD ALS BASISSTRUKTUR FÜR DIE E-SURVEY

Als Teil der Umfrage haben alle Teilnehmer ihre eigene Maturität betreffend IT und OT Sicherheit entlang dem auf NIST Cyber Security Framework (CSF v1.1) basierenden 'IKT Minimalstandard' selbst eingeschätzt. Das NIST CSF besteht aus den folgenden 5 Kategorien ('Capabilities') und 23 Unterkategorien ('Sub-Capabilities').



4. AKTUELLER STAND BETREFFEND CYBER-MATURITÄT | EINTEILUNG ENTLANG VON FÜNF MATURITÄTSSTUFEN

Gemäss ‘IKT Minimalstandard’ wurde die eigene Maturität hierbei pro Unterkategorie in eine von 5 Maturitätsstufen (‘Levels’) durch die Teilnehmenden selbst eingeschätzt. Bemerkung: Maturitätsstufe 0 gilt als «Nicht Umgesetzt».

1

Partiell umgesetzt, nicht vollständig definiert und abgenommen
Risikomanagementprozesse und organisatorische Vorgaben zur IKT-Sicherheit sind nicht formalisiert, und die IKT-Risiken werden üblicherweise nur ad hoc oder reaktiv verwaltet. Ein integriertes Risikomanagementprogramm auf organisatorischer Ebene besteht, aber ein Bewusstsein für IKT-Risiken und ein organisationsweiter Ansatz zur Bewältigung dieser Risiken sind nicht etabliert. Die Organisation verfügt typischerweise nicht über Prozesse, um Informationen zur Cybersecurity innerhalb der Organisation gemeinsam zu nutzen. Ebenso verfügt die Organisation für den Fall eingetretener IKT-Risiken oft nicht über standardisierte Prozesse zum Informationsaustausch oder zur koordinierten Zusammenarbeit mit externen Partnern.

2

Partiell umgesetzt, vollständig definiert und abgenommen
Organisationen, die sich selber auf dem Tier Level 2 einordnen, verfügen typischerweise über Risikomanagementprozesse für IKT-Risiken. Diese sind jedoch nicht als konkrete Handlungsanweisungen implementiert. Auf der organisatorischen Ebene sind IKT-Risiken ins unternehmensweite Risikomanagement integriert, und das Bewusstsein für IKT-Risiken ist auf allen Unternehmensstufen vorhanden. Hingegen fehlen typischerweise unternehmensweite Ansätze zur Steuerung und Verbesserung des Bewusstseins (Awareness) für aktuelle und zukünftige IKT-Risiken. Genehmigte Prozesse und Verfahren sind definiert und umgesetzt. Das Personal verfügt über ausreichende Ressourcen, um seine Aufgaben im Bereich der Cybersecurity wahrzunehmen. Cyber-Security-Informationen werden innerhalb der Organisation auf informeller Basis geteilt. Die Organisation ist sich ihrer Rolle bewusst und kommuniziert mit externen Partnern zum Thema Cybersecurity (z.B. Kunden, Lieferanten, Dienstleistern etc.). Es bestehen jedoch keine standardisierten Prozesse zur Kooperation oder zum Informationsaustausch mit diesen Partnern.

3

Umgesetzt, vollständig oder grösstenteils umgesetzt, statisch
Verfügen über formell genehmigte Risikomanagementpläne und Vorgaben zu deren unternehmensweiten Anwendung. Der Umgang mit IKT-Risiken ist in unternehmensweit gültigen Richtlinien definiert. Die standardisiert erfassten IKT-Risiken sowie die Vorgaben zum Umgang mit denselben werden regelmässig aktualisiert. Dabei werden sowohl Veränderungen der Geschäftsanforderungen berücksichtigt als auch technische Weiterentwicklungen und eine sich verändernde Bedrohungslandschaft, etwa durch neue Akteure oder ein sich wandelndes politisches Umfeld. Prozesse und Verfahren zum Umgang mit veränderten Risiken sind schriftlich definiert. Es werden standardisierte Methoden eingesetzt, um auf Veränderungen der Risiken zu reagieren. Das Personal verfügt über die notwendigen Kenntnisse und Fähigkeiten, um seine Aufgaben zu erfüllen. Die Organisation kennt ihre Abhängigkeiten von externen Partnern und tauscht mit diesen Informationen aus, die Managemententscheidungen innerhalb der Organisation als Reaktion auf Vorfälle ermöglichen.

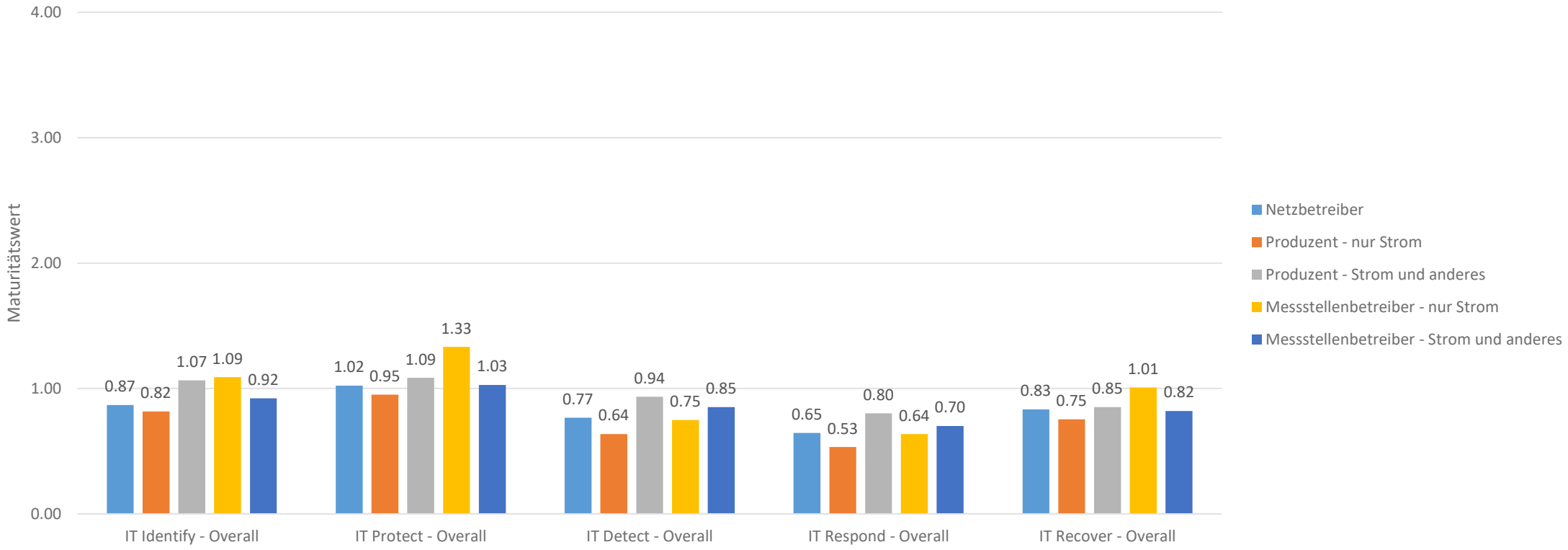
4

Dynamisch, umgesetzt, kontinuierlich überprüft, verbessert
Organisation alle Anforderungen aus den Tier Leveln 1–3 vollständig erfüllt und zusätzlich die eigenen Prozesse, Methoden und Fähigkeiten ständig überprüft und bei Bedarf verbessert. Grundlage zur kontinuierlichen Verbesserung ist eine lückenlose Dokumentation sämtlicher Cybersecurity-Vorfälle. Die Organisation zieht die notwendigen Lehren aus der Analyse vergangener Vorfälle und passt die eigenen Prozesse und eingesetzten Sicherheitstechnologien dynamisch dem neusten Stand der Technik oder sich wandelnden Bedrohungslagen an. IKT-Risikomanagement ist fester Bestandteil der Unternehmenskultur. Erkenntnisse aus vergangenen Vorfällen, Informationen von externen Quellen und aus der permanenten Überwachung der eigenen Systeme und Netzwerke werden fortwährend in den Risikomanagementprozess integriert. Die Organisation teilt laufend Informationen mit Partnern und verfügt dazu über standardisierte Prozesse.

4. AKTUELLER STAND BETREFFEND CYBER-MATURITÄT | AUSWERTUNG

MATURITÄT IT-SICHERHEIT

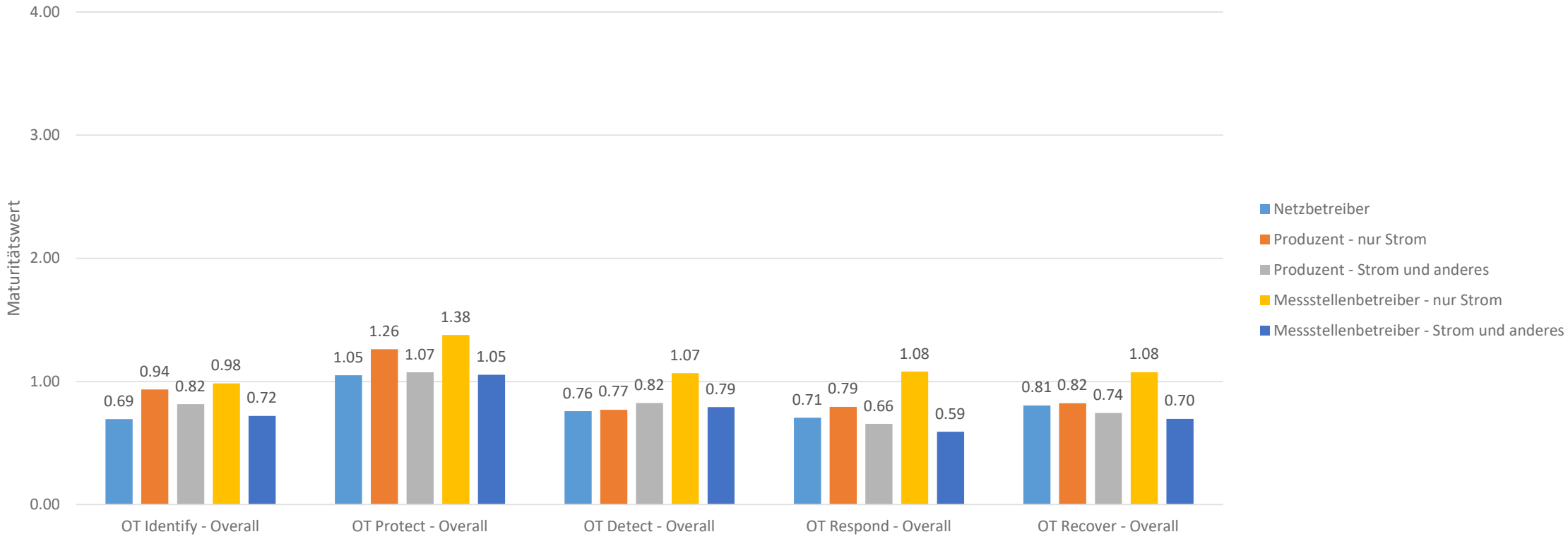
Entlang der 5 NIST Kategorien ergibt sich das folgende Bild über alle 124 Umfrage-Teilnehmer im Bereich der IT Sicherheit. Hierbei ist unter anderem auffällig, dass die aktuelle Maturität in den Bereichen «Identifizieren» und «Schützen» signifikant höher ist (= präventive Massnahmen), als die Fähigkeiten bei der «Erkennung» und der «Reaktion» auf Cyber-Vorfälle, sowie bei der «Erholung» nach einem Vorfall (= Reaktive Fähigkeiten).



4. AKTUELLER STAND BETREFFEND CYBER-MATURITÄT | AUSWERTUNG

MATURITÄT OT-SICHERHEIT

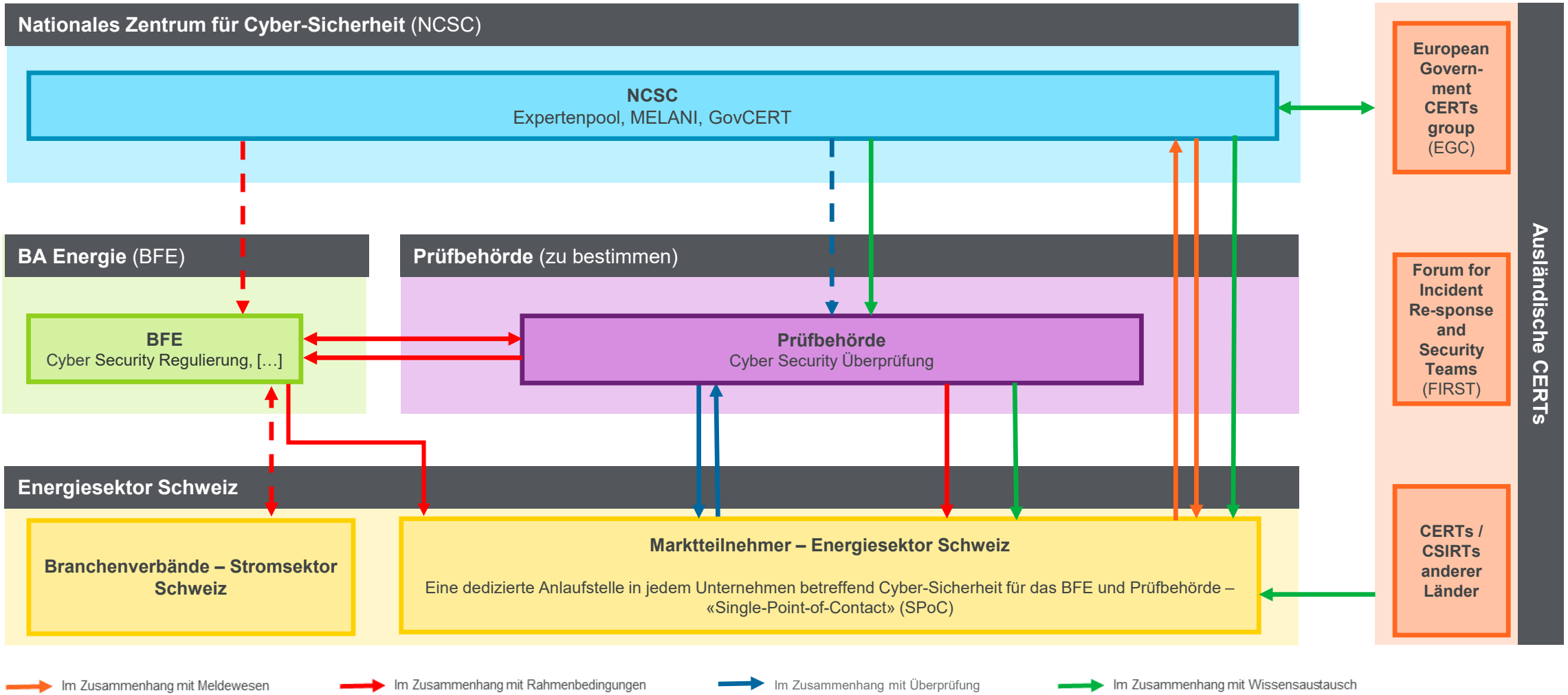
Betreffend OT Sicherheit entlang der 5 NIST Kategorien ergibt sich ein ähnliches Bild. Grundsätzlich glauben die Teilnehmer ihre OT Landschaft etwas besser gehärtet zu haben als ihre IT, die Werte im Bereich «Identifizieren» sind jedoch signifikant tiefer. Dies dürfte u. a. darauf zurückzuführen sein, dass die OT Landschaft und deren Risiken meist lokal direkt vor Ort in den jeweiligen Werken, etc. adressiert werden, jedoch meist keine zentrale Sicht besteht.



5. VORSCHLÄGE ZUR VERBESSERUNG | HANDLUNGSBEDARF

	1. Rahmenbedingungen	2. Überprüfung	3. Meldewesen	4. Wissensaustausch
				
Ziel	*Schaffung einheitlicher, gesetzlicher Rahmenbedingungen in Bezug auf Cyber-Sicherheit und Resilienz*	*Sicherstellung regelmässiger Überprüfung betreffend die Einhaltung reguArialrischer Anforderungen*	*Einführung eines institutionalisierten Meldewesens betreffend laufende Cyber-Vorfälle innerhalb des Sektors*	*Institutionalisierung eines regelmässigen Wissensaustausches betreffend aktuelle Cyber-Gefahren (Threat Intelligence)*
Auszuarbeitende Bereiche	✓ Rechtliche Klärung der Rollen und Verantwortlichkeiten ✓ Identifizierung der zu regulierenden Unternehmen innerhalb des Sektors ✓ (Weiter-)Entwicklung rechtlicher Cyber-Anforderungen	✓ Etablierung einer Prüfbehörde ✓ Etablierung eines zentralen Registers ✓ Überprüfungsmechanismen ✓ Selbstbeurteilungsmechanismen ✓ Sanktionierungs- und Incentivierungsmechanismen	✓ Klare Vorgaben betreffend Meldewesen im Stromsektor ✓ Rechtliche Klärung der Rollen und Verantwortlichkeiten ✓ Zentrale Meldemechanismen und Hilfestellungen für Betroffene	✓ Bereitstellung Sektor-spezifischer Threat Intelligence und konkreter Hilfestellungen für eine adäquate Prophylaxe ✓ Mechanismen zur schnellen und gezielten Weiterverbreitung
	Überblick auf Slide 10	*Überblick auf Slide 11*	*Überblick auf Slide 12*	*Überblick auf Slide 13*

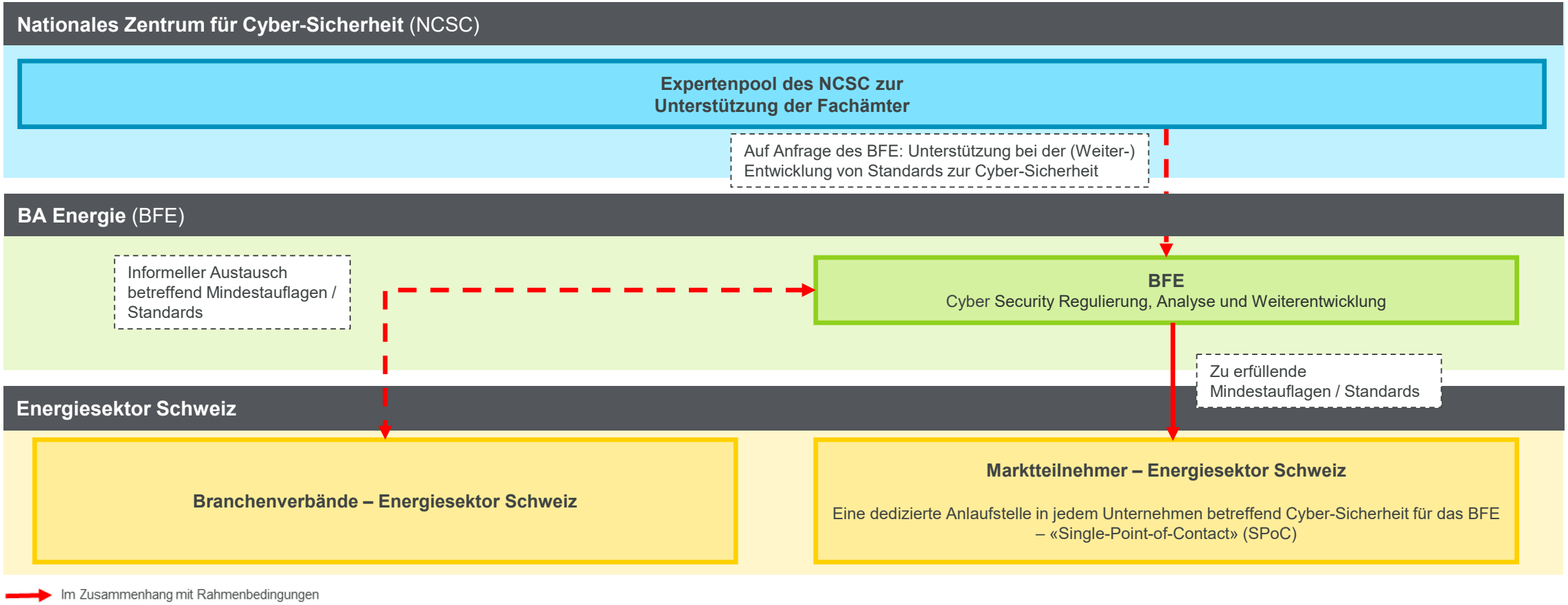
5. VORSCHLÄGE ZUR VERBESSERUNG | GESAMTÜBERBLICK HANDLUNGSBEDARF



5. VORSCHLÄGE ZUR VERBESSERUNG | HANDLUNGSBEDARF

RAHMENBEDINGUNGEN

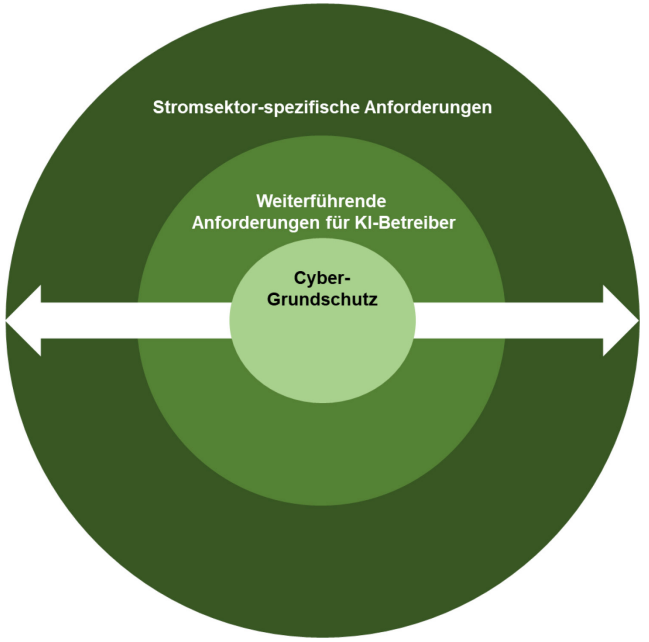
Übersicht betreffend ausgearbeitete Rollen und Verantwortlichkeiten in Bezug auf das Themenfeld #1 «Rahmenbedingungen» – Ziel: Schaffung einheitlicher, gesetzlicher Rahmenbedingungen in Bezug auf Cyber-Sicherheit und Resilienz



5. VORSCHLÄGE ZUR VERBESSERUNG | HANDLUNGSBEDARF RAHMENBEDINGUNGEN

Exkurs: Grundlagen für die Erarbeitung gesetzlich verpflichtender Cyber-Anforderungen

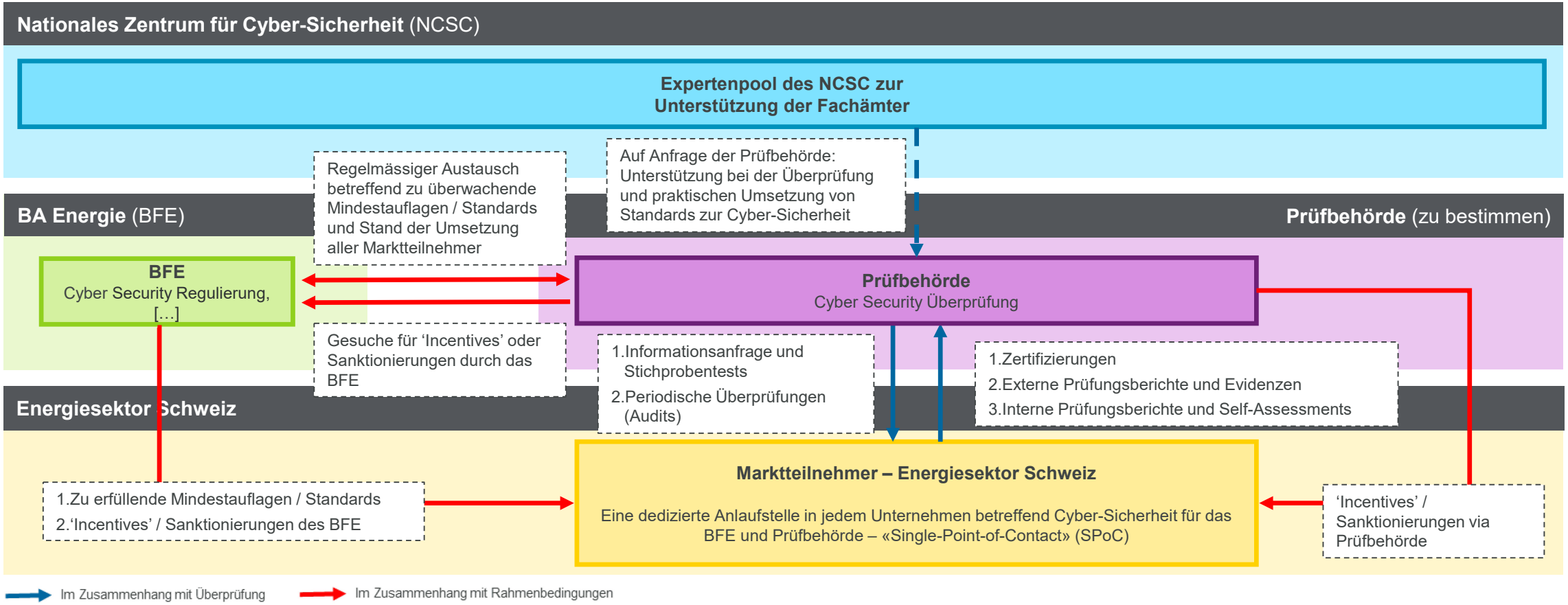
Kategorie	Beschreibung	Beispiele gängiger Referenz-Frameworks und Standards
Allgemeine IT-Sicherheits-Standards für Risiko Management für alle Teilnehmer des Energiesektors Schweiz *Grundstein für Resilienz für Cyber-Sicherheit*	In einem ersten Schritt sollte sichergestellt werden, dass ein gewisser Cyber-Grundschutz für relevante Marktteilnehmer im Schweizer Stromsektor gegeben ist. Hierzu sollten unter anderem auch bereits verfügbare Grundlagen im Bereich der Risikoanalyse berücksichtigt werden	• ISO/IEC 27001 Framework für ISMS • NIST Publikation 800-30 Rev. 1 (Risikomanagement für Informationssysteme) • CRAMM Risikomanagement Methodologie • OCTAVE, Werkzeuge, Techniken und Methoden
Sicherheits-Standards betreffend Cyber-Sicherheit für Betreiber kritischer Infrastrukturen *Anforderungen für KRITS*	In einem zweiten Schritt sollte eine Harmonisierung und Weiterentwicklung der cyber-relevanten Anforderungen für Betreiber kritischer Infrastrukturen innerhalb des Stromsektors Schweiz ins Auge gefasst werden	• ANSI/ISA, Series ISA-62443: Security for industrial automation and control system • NIST Framework für die Verbesserung von Critical Infrastructure Cybersecurity • NERC CIP–002 bis CIP-011 Critical Infrastructure Protection Cyber Security
Spezifische Sicherheits-Standards betreffend Cyber-Sicherheit für den Energiesektor *Berücksichtigung von Sektor-spezifischen Anforderungen*	Sind diese beiden Kategorien zufriedenstellend reguliert, so empfiehlt es sich weiterführenden, Stromsektor-spezifischen Anforderungen zu widmen, welche über den gewünschten Grund-schutz herausgehen	• ISO 27019 Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry • NIST Industrial Control Systems (ICS) Security • IEEE STANDARD 1402-2000 • IEC 61850 Power Utility Automation



Fazit: Bei der Erarbeitung neuer gesetzlich verpflichtender Cyber- und Resilienz-Anforderungen für den Sektor sollte grundsätzlich stets zuerst an bereits bestehenden, nationalen und kantonalen Regulierungen angeknüpft werden und diese wo sinnvoll harmonisieren und/oder referenzieren. Wenn immer möglich sollte auch eine Referenzierung mit gängigen, internationalen Standards in Betracht gezogen werden.

5. VORSCHLÄGE ZUR VERBESSERUNG | HANDLUNGSBEDARF ÜBERPRÜFUNG

Übersicht betreffend ausgearbeitete Rollen und Verantwortlichkeiten in Bezug auf das Themenfeld #2 «Überprüfung» – Ziel: Sicherstellung regelmässiger Überprüfung betreffend die Einhaltung reguArialrischer Anforderungen



5. VORSCHLÄGE ZUR VERBESSERUNG | HANDLUNGSBEDARF ÜBERPRÜFUNG

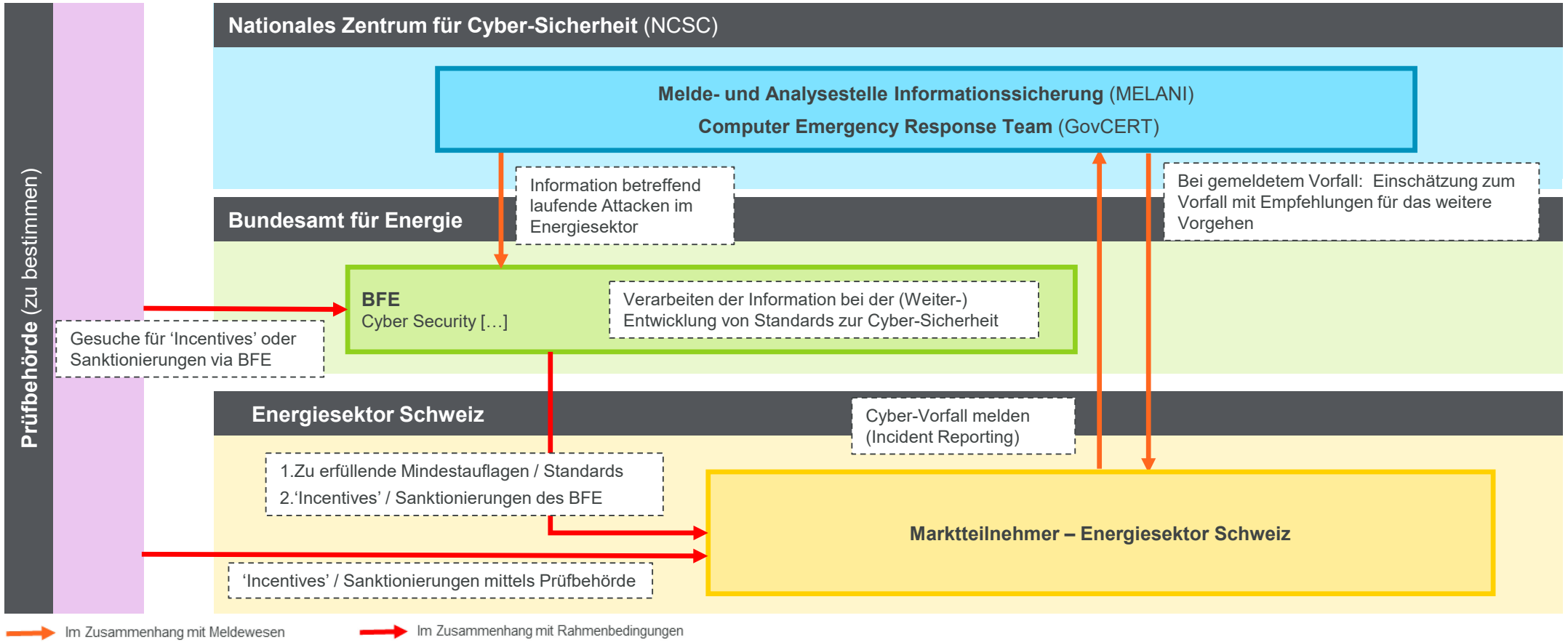
Exkurs: Optionen zur Festlegung der Prüfbehörde

#	Option	Vorteile	Nachteile
1	**BFE als Prüfbehörde** (keine dedizierte Prüfbehörde)	+ BFE übernimmt bereits heute teilweise Aufgaben, welche sowohl in den Bereich der Aufsicht, als auch in die anschliessende Überprüfung fallen + Ein gewisses Fachwissen im Bereich Cyber-Sicherheit und Digitalisierung ist beim BFE bereits vorhanden, jedoch ausbaubedürftig + BFE verfügt über gewisse Sanktionierungs- und 'Incentivierungs'-Kompetenzen und ist bereits heute zuständige Instanz bei Verstössen gegen das StromVG	– Keine klare Gewaltentrennung zwischen regulierender und überprüfender Instanz – Entspricht derzeit nicht dem aktuellen Mandat des BFE im Bereich der Stromversorgung – Dieser Ansatz würde vermehrt zu Kompetenz-Abgrenzungsfragen zwischen dem BFE und den aktuellen Tätigkeiten der ElCom führen
2	**ElCom als Prüfbehörde** (dedizierte Prüfbehörde)	+ Entspricht bereits heute teilwiese dem aktuellen Mandat der ElCom, welche für die Überwachung der Einhaltung des StromVG durch Netzbetreiber zuständig ist + ElCom verfügt bereits heute über gewisse Kompetenzen, Prozesse und Mechanismen, welche sich künftig für eine überwachende Funktion betreffend Cyber-Sicherheit und Resilienz im Schweizer Stromsektor weiterverwenden lassen würden + Klare Gewaltentrennung zwischen der regulierende und der überwachenden Instanz + ElCom verfügt bereits über detaillierte Branchekenntnisse, ist mit einem Grossteil der Marktteilnehmer gut vernetzt und eingespielt	– Es besteht grosses Fachwissen im Bereich der Kostenregulierung innerhalb der ElCom, je-doch noch kaum relevantes Wissen in den Bereichen der Cyber-Sicherheit und Resilienz – Gewisse Doppelspurigkeiten mit dem aktuellen Mandat des Eidgenössischen Instituts für Metrologie (METAS), welches aktuell bereits überprüfende Tätigkeiten betreffend die Einhaltung von sicherheitstechnischen Anforderungen an Smart Meter wahrnimmt
3	**METAS als Prüfbehörde** (dedizierte Prüfbehörde)	+ Entspricht bereits heute teilwiese dem aktuellen Mandat des METAS, welches für die Überwachung der sicherheitstechnischen Anforderungen von Smart Meter zuständig ist + METAS verfügt bereits heute über gewisse überwachende Prozesse und Mechanismen + Klare Gewaltentrennung zwischen der regulierenden und der überwachenden Instanz + METAS verfügt bereits über detaillierte Kenntnisse, in einem Teilbereich der Cyber-Sicherheit innerhalb des Schweizer Stromsektors und ist mit einem Grossteil der Marktteilnehmer bereits gut vernetzt und eingespielt	– Es besteht ein gewisses Fachwissen im Bereich der Cyber-Sicherheit innerhalb des METAS, jedoch benötigtes es noch eine deutliche Ausweitung der aktuellen Kenntnisse und Kompetenzen – Gewisse Doppelspurigkeiten mit dem aktuellen Mandat der ElCom, welche aktuell bereits für überprüfende Tätigkeiten betreffend die Einhaltung des StromVG durch Netzbetreiber zuständig ist

Fazit: Optionen 2 oder 3 erscheinen als sinnvolle Vorgehensweise für die Schweiz. Eine dedizierte Prüfbehörde sichert eine Gewaltentrennung zwischen der regulierenden, sowie der überwachenden Instanz. Beide Optionen entsprechen bereits heute teilweise den aktuellen Mandaten der jeweiligen Organe, was den zukünftigen Implementationsaufwand vereinfachen würde.

5. VORSCHLÄGE ZUR VERBESSERUNG | HANDLUNGSBEDARF MELDEPFLICHT

Übersicht betreffend ausgearbeitete Rollen und Verantwortlichkeiten in Bezug auf das Themenfeld #3 «Meldewesen» – Ziel: Einführung eines institutionalisierten Meldewesens betreffend laufende Cyber-Vorfälle innerhalb des Sektors



5. VORSCHLÄGE ZUR VERBESSERUNG | HANDLUNGSBEDARF MELDEPFLICHT

Exkurs: Ausgestaltung des Meldewesens innerhalb des Sektors

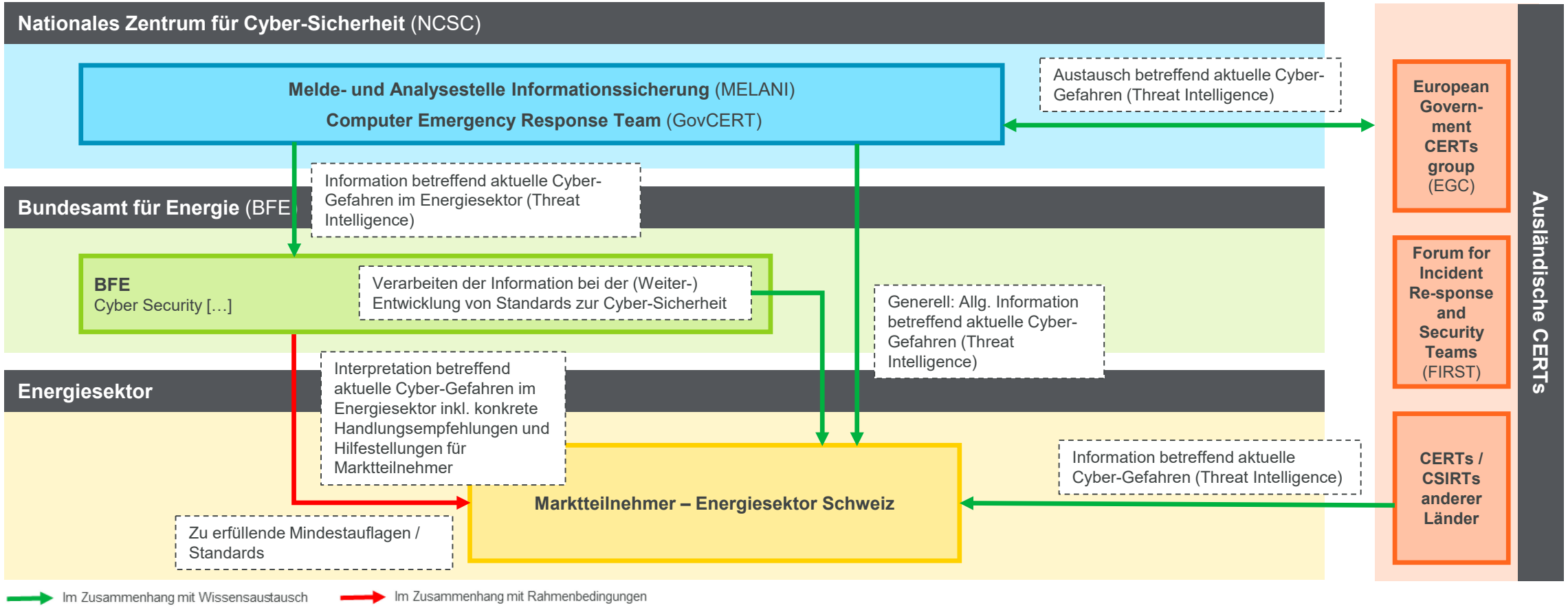
#	Option	Vorteile	Nachteile
1	**Meldepflicht – Anonym:** Marktteilnehmer des Energiesektors Schweiz werden gesetzlich verpflichtet, Meldungen von Vorfällen an das NCSC durchzuführen. Meldungen werden anonym an das NCSC übertragen, werden dann weiter vertraulich weiterbehandelt und Betroffene nicht namentlich an die Prüfstelle zurückgemeldet	+ Verbesserung der internen Detektions- und Rapportierungsprozesse der Unternehmen, um Meldepflicht nachzukommen + Verbesserung der Beurteilung der effektiven Bedrohungslage mittels Transparenz aller laufenden Attacken im Energiesektor Schweiz – kann bei künftigen Regulationen und 'Incentivierungen' mitberücksichtigt werden + Garantierte Hilfestellung des NCSC für alle betroffenen Unternehmen im Falle eines Cyber-Vorfalls, sowie Früherkennung von Angriffsmustern durch die zentrale Informationskonsolidierung zu Bedrohungen und Möglichkeit koordiniert reagieren zu können	– Teilweise zusätzliche Aufwände bei Marktteilnehmern, um die benötigte Maturität zu erreichen, damit Cyber-Sicherheitsvorfälle entsprechend erkannt und gemeldet werden können – Durch die Zusicherung des NCSC, Meldungen anonym zu behandeln, wird dem BFE die Möglichkeit genommen, allenfalls betroffenen Marktteilnehmern künftig gezielt weitere Massnahmen aufzuerlegen und/oder weiterführende Sanktionen umzusetzen
2	**Meldepflicht – Nicht Anonym:** Analog Option 1 – jedoch wird das BFE auch erfahren, welches die betroffenen Unternehmen sind	+ Gleiche Vorteile wie bei Option 1 + Zusätzlich: Möglichkeit für das BFE, allenfalls betroffenen Marktteilnehmern künftig gezielt weitere Massnahmen aufzuerlegen und/oder weiterführende Sanktionen umzusetzen	– Teilweise zusätzliche Aufwände bei Marktteilnehmern, um die benötigte Maturität zu erreichen – Höherer Aufwand auf staatlicher Seite zur Etablierung einer Struktur zu regelmässigem Informationsaustausch zwischen dem NCSC und dem BFE, sowie zusätzliche Aufwände auf Seite des BFE bei der weiterführenden Analyse der gemeldeten Vorfälle
3	**Keine Meldepflicht:** Keine Änderung des bestehenden Ansatzes für die Schweiz	+ Keine Veränderung der heutigen Situation und somit keine Erhöhung der Aufwände für alle Beteiligten	– Verzicht auf alle oben genannten Vorteile der Optionen 1 und 2

Fazit: Unter Berücksichtigung der genannten Vor- und Nachteile, sowie der ergriffenen Massnahmen des Umlandes zum Schutz kritischer Infrastruktur (Umsetzung der NIS-Richtlinie), wird eine Meldepflicht als sinnvoll erachtet und wäre ein wertvoller Beitrag zur NCS 2018-2022. Basierend auf den Befundnissen der bundesrätlichen Expertenkommission zur Zukunft von Datenschutz und Datensicherheit sprach sich der Bundesrat Ende 2020 Bundesrat ebenfalls für eine Meldepflicht für kritische Infrastrukturen bei Cyberangriffen aus. Das Thema wird aktuell innerhalb einer BFE Arbeitsgruppe entsprechend weiter ausgearbeitet.

5. VORSCHLÄGE ZUR VERBESSERUNG | HANDLUNGSBEDARF

WISSENSAUSTAUSCH

Übersicht betreffend ausgearbeitete Rollen und Verantwortlichkeiten in Bezug auf das Themenfeld #4 «Wissensaustausch» – Ziel: Institutionalisierung eines regelmässigen Wissensaustausches betreffend aktuelle Cyber-Gefahren (Threat Intelligence)



DISKUSSION & FRAGEN

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesamt für Energie BFE
Office fédéral de l'énergie OFEN
Ufficio federale dell'energia UFE
Uffizi federal d'energia UFE

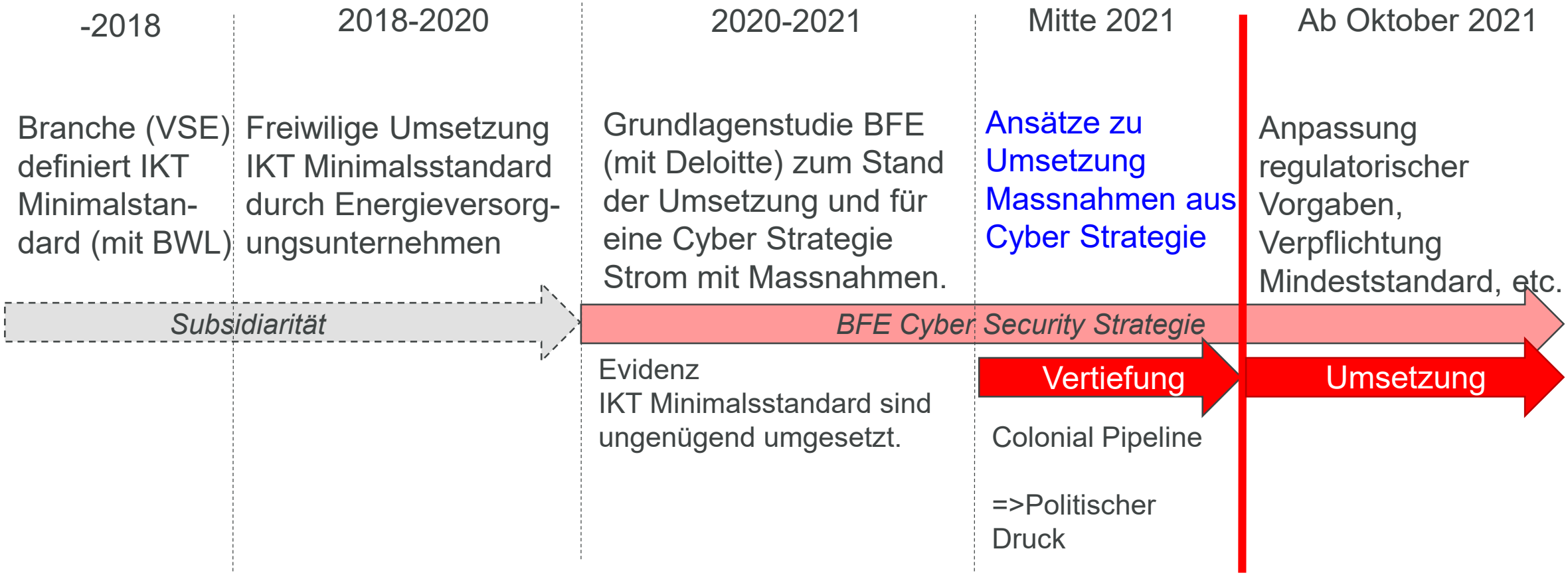
STRATEGIE CYBER SECURITY & RESILIENZ
AUSBLICK ZUR UMSETZUNG DER MASSNAHMEN

BUNDESAMT FÜR ENERGIE ▪ DIGITAL INNOVATION OFFICE ▪ 22. SEPTEMBER 2021

CYBER SECURITY IN DER POLITIK LÖSUNGEN SIND GEFORDERT

- **Postulat 17.3475** Graf-Litscher
  «Meldepflicht bei schwerwiegenden Sicherheitsvorfällen bei kritischen Infrastrukturen». Angenommen.
- **Postulat 18.4197** Wasserfallen
  «IT-Sicherheit kritischer Infrastrukturen. Welche Mittel und Massnahmen ergreift der Bundesrat?» Angenommen
- **Postulat 19.3136** Dobler
  «Haben wir die Hard- und Softwarekomponenten bei unseren kritischen Infrastrukturen im Griff?». Angenommen

STRATEGIE CYBER SECURITY STROM STAND DER DINGE



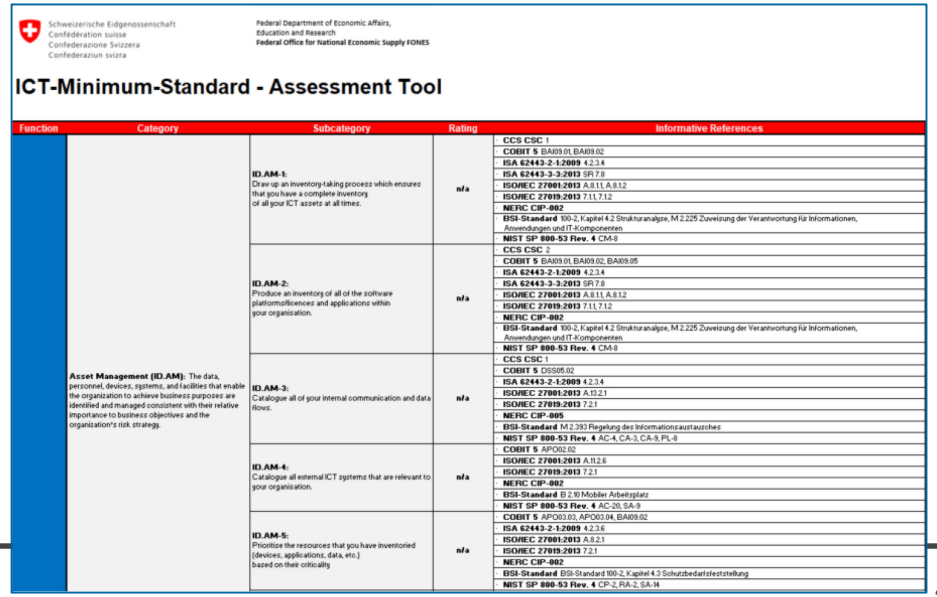
MASSNAHMEN CYBER SECURITY STRATEGIE WICHTIGE VERTIEFUNGEN

- Wie können Schnittstellen zwischen BFE, NCSC, ElCom, BWL verbessert werden?
- Welchen Minimalstandard müsste man verpflichten und welches Niveau braucht es?
- Wie kann die Umsetzung des Mindeststandards verifiziert werden?
- Inwieweit ist «One Size Fits All" machbar oder wie sieht ein abgestuftes System aus?
- Wie können Anreize gesetzt und die Sensibilisierung der Unternehmen erhöht werden?
- Wie sieht eine Meldepflicht zu Cyber Security in der Stromversorgung aus?
- …

WELCHER STANDARD ALS MINIMALSTANDARD? DIE ROLLE DES IKT MINIMALSTANDARDS

Norm	Beschreibung
ISO 38500	IT-Governance durch das Unternehmen
ISO 31000	Risikomanagement
ISO 27001	Umsetzung des Sich. Management System
ISO 27002	Verwalten von Sicherheitsrisiken
ISO 27019	Für Steuerung-Systemen
ITIL	Für Produktions-und-Support von IT
CMMi	Für die Entwicklung, 5 Reifegrade
TOGAF	IT-Unternehmensarchitektur
COBIT 5	Die 11 Vektoren zur Verbesserung der IT-Governance
RiskIT	Governance, Risikobewertung und -reaktion
ValIT	Projektportfoliomanagement
NERC	North American Electric Reliability Corporation
CPNI/NCSC	Centre for the Protection of National Infrastructure
MEHARI	Risikoanalyse und -behandlung
….	

Was macht Sinn für die Branche?
Arbeitsgruppe IKT Minimalstandard
(BWL, BFE, …)



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Economic Affairs, Education and Research
Federal Office for National Economic Supply FONES

ICT-Minimum-Standard - Assessment Tool

Function	Category	Subcategory	Rating	Informative References
	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1:** Draw up an inventory-taking process which ensures that you have a complete inventory of all your ICT assets at all times.	n/a	**CCS CSC** 1 **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **ISO/IEC 27019:2013** 7.1.1, 7.1.2 **NERC CIP-002** **BSI-Standard** 100-2, Kapitel 4.2 Strukturanalyse, M 2.225 Zuweisung der Verantwortung für Informationen, Anwendungen und IT-Komponenten **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-2: Produce an inventory of all of the software platforms/licences and applications within your organisation.	n/a	**CCS CSC** 2 **COBIT 5** BAI09.01, BAI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **ISO/IEC 27019:2013** 7.1.1, 7.1.2 **NERC CIP-002** **BSI-Standard** 100-2, Kapitel 4.2 Strukturanalyse, M 2.225 Zuweisung der Verantwortung für Informationen, Anwendungen und IT-Komponenten **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-3: Catalogue all of your internal communication and data flows.	n/a	**CCS CSC** 1 **COBIT 5** DSS05.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISO/IEC 27001:2013** A.13.2.1 **ISO/IEC 27019:2013** 7.2.1 **NERC CIP-005** **BSI-Standard** M 2.393 Regelung des Informationsaustausches **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: Catalogue all external ICT systems that are relevant to your organisation.	n/a	**COBIT 5** APO02.02 **ISO/IEC 27001:2013** A.11.2.6 **ISO/IEC 27019:2013** 7.2.1 **NERC CIP-002** **BSI-Standard** B 2.10 Mobiler Arbeitsplatz **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Prioritise the resources that you have inventoried (devices, applications, data, etc.) based on their criticality.	n/a	**COBIT 5** APO03.03, APO03.04, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.6 **ISO/IEC 27001:2013** A.8.2.1 **ISO/IEC 27019:2013** 7.2.1 **NERC CIP-002** **BSI-Standard** BSI-Standard 100-2, Kapitel 4.3 Schutzbedarfsfeststellung **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14

IKT MINIMALSTANDARD VERBESSERUNGSPOTENTIAL

IKT-Minimalstandard

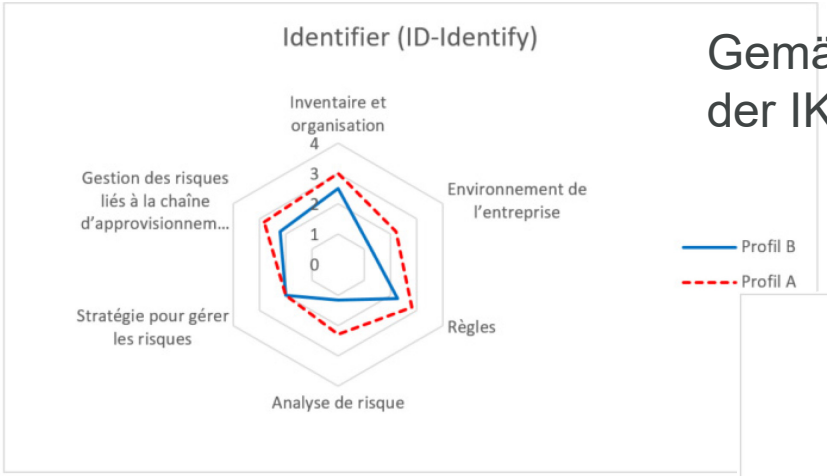
Die IKT Minimalstandards sind in mehrere Branchen definiert und akzeptiert. Was heute fehlt:

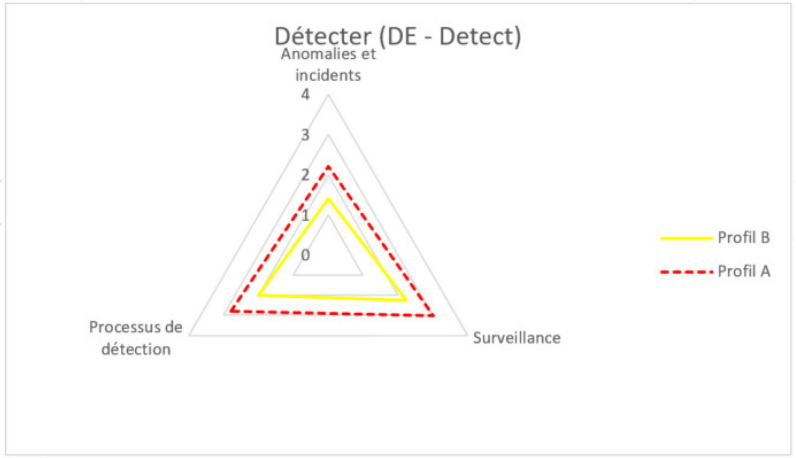
a) Verpflichtung => Anpassung der Verordnungen
b) Schutzniveau zu erreichen (SOLL-Profil)
c) Verifizierung/Prüfung

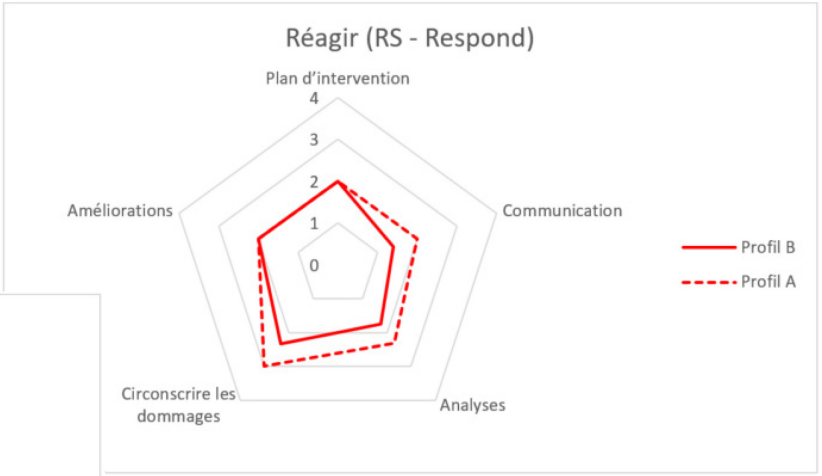
Strom | Trinkwasser | Lebensmittel | Abwasser | Gas | ÖV | Fernwärme

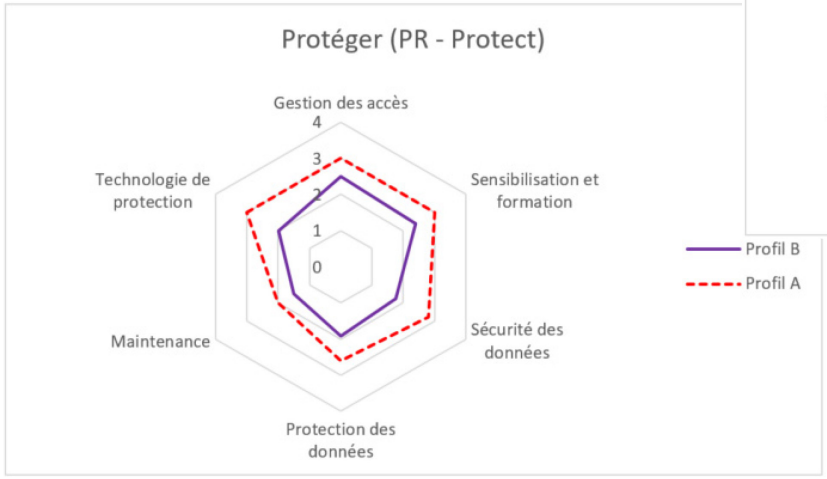
CYBERSCHUTZ NIVEAU FÜR MINIMALSTANDARD UNTERSCHIEDLICHE SOLL-PROFILE

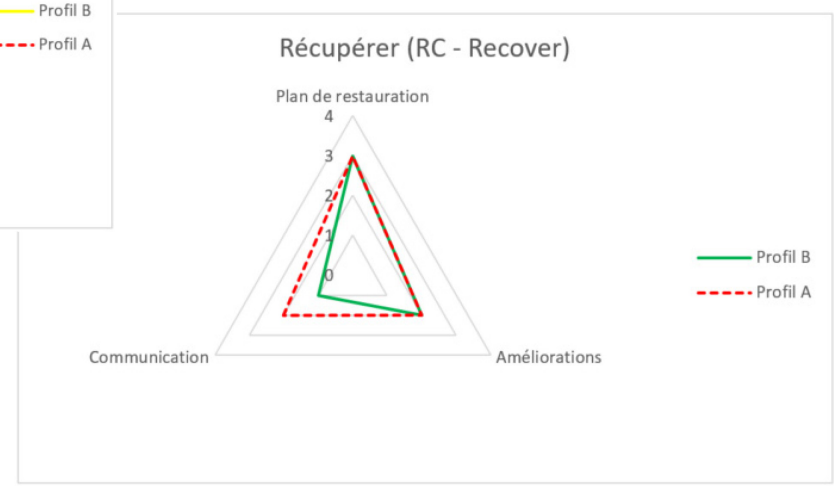
Gemäss das Assessment Tool der IKT Minimal Standards:











MELDEPFLICHT CYBERVORFÄLLE ANPASSUNGEN BEREITS AUF DEM WEG

- Anpassungen des ISG Vernehmlassung 2022.
- Grundlagen Stromversorgung durch BFE. Mitwirkung VSE.
- Aufteilung Unternehmen Elektrizitätswirtschaft in 2 Gruppen.
- Profil A (hat Meldepflicht) und Profil B (keine Meldepflicht).
- Profil A: NE 1-4 oder 50MWh/4 Stunden bzw. 20'000 Kunden.

ZUSAMMENFASSUNG AUSBLICK

- Der IKT Minimalstandard ist im Energiesektor seit 2018 bekannt. Grundlage für verpflichtenden Minimalstandard.
- Überprüfung minimalinvasiv. Audit einfacher als Zertifizierung.
- Audit kombiniert mit regelmässiger Selbsteinschätzung und Stichproben.
- Keine «One Size Fits All» Lösung. Wie bei Meldepflicht 2 Gruppen.
- Anpassung von gesetzlichen Rahmenbedingungen wird geprüft.
- Benennung von IT/OT Verantwortlichen pro Unternehmen notwendig.

DISKUSSION & FRAGEN

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesamt für Energie BFE
Office fédéral de l'énergie OFEN
Ufficio federale dell'energia UFE
Uffizi federal d'energia UFE

VERDANKUNG