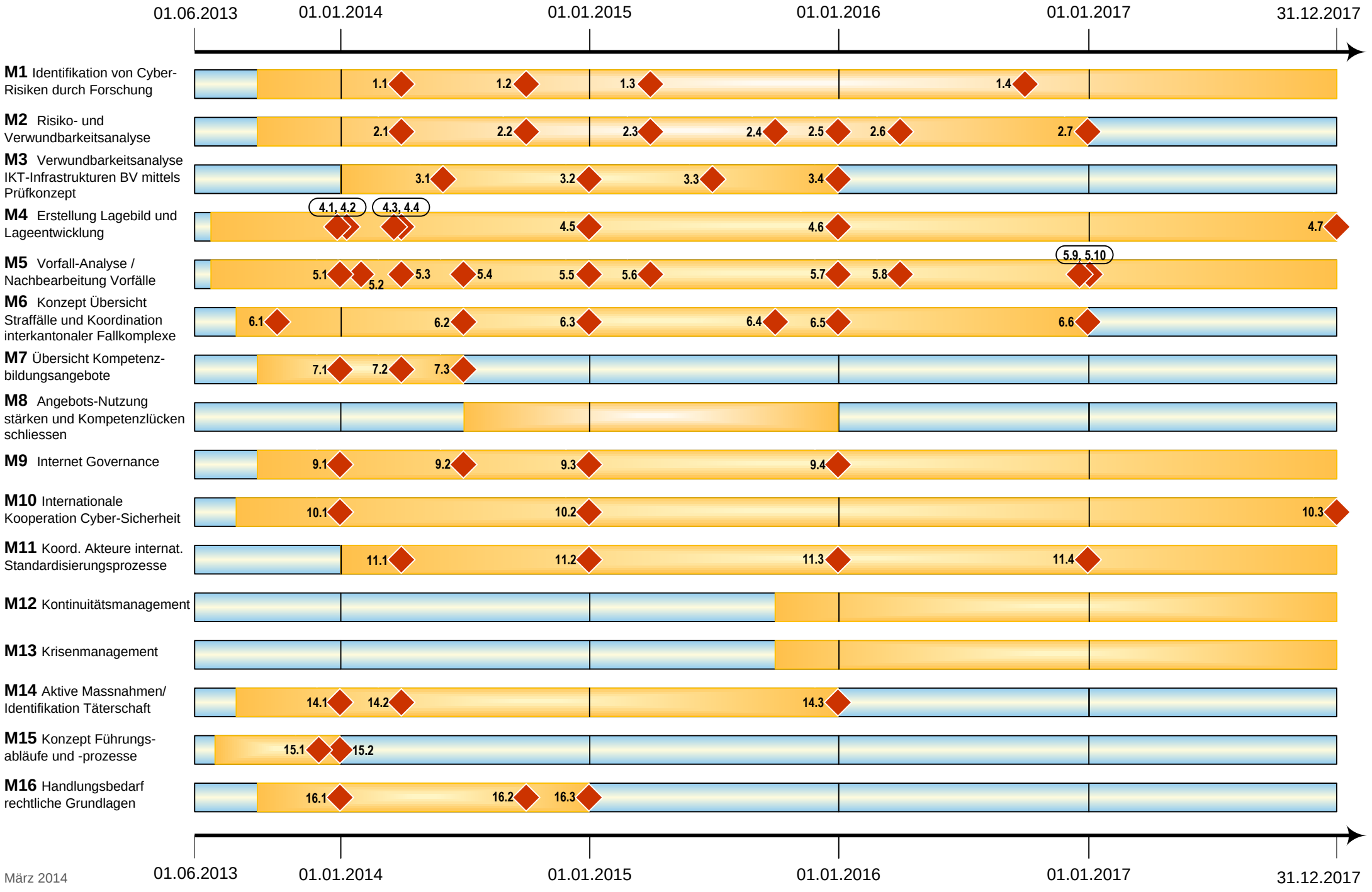
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Informatiksteuerungsorgan des Bundes ISB
Melde- und Analysestelle Informationssicherung MELANI

Roadmap NCS



Roadmap NCS: Ziele und Meilensteine

Mass-nah-men	**Ziele**	**Meilensteine**	**Federführung** und Partner	**Abstimmung mit:** A) Risikopolitik des Bundes B) SKI-Strategie C) Strategie Informations-gesellschaft
M 1	**Identifikation von Cyber-Risiken durch Forschung** Die verantwortlichen Bundesstellen tauschen sich untereinander und mit Akteuren ausserhalb der Bundesverwaltung zu aktuellen und zu erforschenden Entwicklungen im In- und Ausland im Zusammenhang mit Cyber-Risiken aus und treiben bei Bedarf intramuros Forschung oder erteilen Forschungsaufträge.	**MS 1.1** März 2014: Aktuell wichtigste Forschungsthemen sind im Austausch mit Expertinnen und Experten identifiziert. **MS 1.2** September 2014: Organisationsstruktur für Auftraggeber von Forschungsvorhaben und Austausch-Prozesse sind etabliert. **MS 1.3** März 2015: Prozesse zur Identifikation von Entwicklungen und Forschungsbedarf betreffend Cyber-Risiken sind erstellt. **MS 1.4** September 2016: Ergebnis der Analyse der Wirkung der in M1 definierten Prozesse und involvierten Akteure liegt vor.	**verantwortliche Bundesstellen;** Koordination durch KS NCS	C)

Mass-nah-men	Ziele	Meilensteine	Federführung und Partner	Abstimmung mit: A) Risikopolitik des Bundes B) SKI-Strategie C) Strategie Informations-gesellschaft
M 2	**Risiko- und Verwundbarkeitsanalyse** In den 28 kritischen Teilsektoren[1] sind in Zusammenarbeit mit den entsprechenden Fachbehörden und Verbänden sowie unter Einbezug der IKT-Leistungserbringer und Systemlieferanten Risiko- und Verwundbarkeitsanalysen durchgeführt worden. Diese sind nach einem möglichst einheitlichen Ansatz erfolgt. Die Ergebnisse der Risiko- und Verwundbarkeitsanalysen wurden in Zusammenarbeit mit MELANI zu einer gesamtheitlichen Analyse der Bedrohungslage konsolidiert. Die Ergebnisse dienen insbesondere als Grundlage der Arbeiten zur Erfüllung der Massnahmen 12 und 13.	**MS 2.1** März 2014: Methodik und Vorgehen sind definiert und zwischen BABS und BWL abgesprochen. **MS 2.2** September 2014: Voranalyse für die 1. Gruppe der kritischen Teilsektoren ist abgeschlossen. **MS 2.3** März 2015: Voranalyse für die 2. Gruppe der kritischen Teilsektoren ist abgeschlossen. **MS 2.4** September 2015: Risiko- und Verwundbarkeitsanalyse für die 1. Gruppe der kritischen Teilsektoren ist abgeschlossen. **MS 2.5** Dezember 2015: Voranalyse für die 3. Gruppe der kritischen Teilsektoren ist abgeschlossen. **MS 2.6** März 2016: Risiko- und Verwundbarkeitsanalyse für die 2. Gruppe der kritischen Teilsektoren ist abgeschlossen. **MS 2.7** Dezember 2016: Risiko- und Verwundbarkeitsanalyse für die 3. Gruppe der kritischen Teilsektoren ist abgeschlossen.	**BWL, BABS; Fachbehörden/ Regulatoren**; MELANI	A) und B)

[1] Gemäss Umsetzungsplan NCS (S. 4, FN 1 und 2): Die 13 Teilsektoren des BWL sind: Energie (Erdgasversorgung, Erdölversorgung, Stromversorgung), Industrie (Chemie- und Heilmittelindustrie, Maschinen- Elektro- und Metallindustrie); Information und Kommunikation (Informationstechnologien, Telekommunikation); Nahrung (Lebensmittelversorgung, Wasserversorgung); Verkehr (Luftverkehr, Schienenverkehr, Schiffsverkehr, Strassenverkehr).
Die 15 Teilsektoren des BABS sind: Behörden (Parlament, Justiz, Verwaltung; Forschung und Lehre, Kulturgüter, internationale Organisationen); Entsorgung (Abwasser, Abfallentsorgung); Finanzen (Banken, Versicherungen); Gesundheit (Ärztliche Betreuung und Spitäler, Labors); Information und Kommunikation (Medien, Postverkehr); Öffentliche Sicherheit (Armee, Blaulichtorganisationen, Zivilschutz).

Mass-nah-men	Ziele	Meilensteine	Federführung und Partner	Abstimmung mit: A) Risikopolitik des Bundes B) SKI-Strategie C) Strategie Informations-gesellschaft
M 3	**Verwundbarkeitsanalyse IKT-Infrastrukturen Bundesverwaltung mittels Prüfkonzept** Die Verantwortlichen der Generalsekretariate und die zuständigen Leistungserbringer haben die IKT-Infrastrukturen der Bundesverwaltung anhand eines Prüfkonzepts auf systemische, organisatorische, und technische Verwundbarkeiten hin untersucht und die IT-Risiken erkannt. Die Erarbeitung und Umsetzung des Prüfkonzepts ist mit Unterstützung des BIT und der FUB erfolgt und wurde mit laufenden Projekten koordiniert. Die Ergebnisse sind in Zusammenarbeit mit MELANI zu einer gesamtheitlichen Analyse der Bedrohungslage konsolidiert. Das Prüfkonzept identifiziert die IT-Risiken für jeden kritischen Prozess gemäss SKI-Leitfaden, definiert die jeweils systemrelevanten Mindeststandards und integriert die IT-Risiken in das Gesamtrisiko jedes kritischen Prozesses. Die Kantone, die Wirtschaft und die KI-Betreiber erhalten bei Interesse dieses Prüfkonzept der IKT-Infrastrukturen der Bundesverwaltung zur Verwendung für die eigenen Verwundbarkeits-Überprüfungen.	**MS 3.1** Mai 2014: Konzept für die Erstellung eines Prüfkonzepts und dessen Umsetzung ist durch die Interessenvertreter genehmigt. **MS 3.2** Dezember 2014: Entwurf des Prüfkonzepts liegt vor. **MS 3.3** Juni 2015: Die Umsetzungs-Machbarkeit des Prüfkonzeptentwurfs ist durch die zuständigen LE (FUB, BIT) und die verantwortlichen GS der Departemente überprüft. **MS 3.4** Dezember 2015: Prüfkonzept liegt vor, und die Evaluation, ob es der Wirtschaft und den Kantonen als Empfehlung abgegeben werden kann, ist abgeschlossen. Vorbereitung zur Konzeptumsetzung sind abgeschlossen.	**ISB**; BIT, FUB, MELANI	B)

Mass-nah-men	**Ziele**	**Meilensteine**	**Federführung** und Partner	**Abstimmung mit:** A) Risikopolitik des Bundes B) SKI-Strategie C) Strategie Informations-gesellschaft
M 4	**Erstellung Lagebild und Lageentwicklung** Die relevanten und verantwortlichen Akteure aus Politik, Wirtschaft und Gesellschaft können sich über Vorfälle von nationaler Bedeutung und besonderer Relevanz informieren. Es werden ihnen dazu stufengerecht für die jeweiligen Verantwortungsbereiche aufgearbeitete Analysen zur Verfügung gestellt, die über das Lagebild und die Lageentwicklung Auskunft geben. Diese Erkenntnisse wurden im Rahmen des Public Private Partnership-Modells von MELANI gesammelt, bewertet, analysiert und in einer Lagedarstellung fusioniert. Das notwendige Cyber-Spezialwissen und die technischen Kapazitäten wurden dazu ausgebaut, wie auch die Plattform für den freiwilligen Informationsaustausch mit ausgewählten KI-Betreibern und der Wirtschaft gestärkt.	**MS 4.1** Dezember 2013: Konzept zur Stärkung von MELANI als Plattform für den Informationsaustausch ist erstellt. **MS 4.2** Dezember 2013: Cyberaspekte des Auftrags NDB sind identifiziert und die Organisationsstruktur ist definiert. **MS 4.3** März 2014: Service Level Agreement (SLA) zusammen mit FUB-ZEO ist angepasst. **MS 4.4** März 2014: Neue Prozesse des Informationsaustausches zur Bedrohungs- und Risikolage im Cyber-Bereich sind definiert. **MS 4.5** Dezember 2014: Zusammenarbeit zwischen MELANI-ISB/ GovCERT, MELANI-OIC und Cyber NDB ist etabliert. **MS 4.6** Dezember 2015: Spezialwissen und Fähigkeiten im Cyber-Bereich sind beim NDB aufgebaut mit FUB und MND als Leistungserbringer. **MS 4.7** Dezember 2017: Konzept zur Stärkung von MELANI als Plattform für den Informationsaustausch ist umgesetzt.	**MELANI, NDB;** KOBIK, FUB, MND, BIT	

Mass-nah-men	Ziele	Meilensteine	Federführung und Partner	Abstimmung mit: A) Risikopolitik des Bundes B) SKI-Strategie C) Strategie Informations-gesellschaft
M 5	**Vorfall-Analyse und Nachbearbeitung von Vorfällen** Der Bund, die Kantone und die KI-Betreiber haben ihre eigenen Massnahmen im Umgang mit Vorfällen überprüft und weiterentwickelt. Die Erkenntnisse aus relevanten Vorfällen (Incident durch Malware, Botnetze, Trojaner) werden an MELANI weitergegeben, wozu bundesinterne und -externe Prozesse etabliert sind. Bei der Nachbearbeitung relevanter Vorfälle werden KI-Betreiber und IKT-Leistungserbringer, auf Wunsch, von MELANI technisch unterstützt. Erkenntnisse zu Staatsschutz relevante Vorfällen im Zusammenhang mit Cyber-Risiken werden vom NDB an MELANI weitergegeben. Die technischen Kapazitäten zur Überwachung der Bundesnetze sind innerhalb der Dienstleistungserbringer (CERTs) aufgebaut. Plattformen und Infrastrukturen zur Erkennung und Eindämmung von Cyber Bedrohungen, sowie technische Unterstützung der kritischen Infrastrukturbetreibern sind etabliert. Ebenfalls ausgebaut sind bei den relevanten Bundesstellen das Spezialwissen und die forensischen Fähigkeiten zur Erkennung und Bekämpfung von Cyber Bedrohungen.	**MS 5.1** Dezember 2013: Cyberaspekte des Auftrags im NDB sind identifiziert und die Organisationsstruktur ist definiert. **MS 5.2** Januar 2014: Organisationsstruktur im GovCERT ist definiert **MS 5.3** März 2014: 1. Phase zur Erhöhung der Durchhaltefähigkeit im im GovCERT ist abgeschlossen. **MS 5.4** Juni 2014: Plattform zur Nachbearbeitung von Vorfällen ist etabliert. **MS 5.5** Dezember 2014: Infrastruktur zur Erkennung von Malware Aktivitäten bei ausgewählten kritischen Infrastrukturbetreibern ist aufgebaut. **MS 5.6** März 2015: 2. Phase zur Erhöhung der Durchhaltefähigkeit im GovCERT ist abgeschlossen. **MS 5.7** Dezember 2015: Plattform zur sicheren und zeitnahen Kommunikation zur technischen Unterstützung mit ausgewählten kritischen Infrastrukturbetreibern ist aufgebaut. **MS 5.8** März 2016: 3. Phase zur Erhöhung der Durchhaltefähigkeit im GovCERT ist abgeschlossen.	**MELANI, NDB;** FUB, MND, BIT	

Mass-nah-men	Ziele	Meilensteine	Federführung und Partner	Abstimmung mit: A) Risikopolitik des Bundes B) SKI-Strategie C) Strategie Informations-gesellschaft
		MS 5.9 Dezember 2016: Bundesinterne und -externe Prozesse zur Weitergabe von Erkenntnissen an MELANI sind etabliert. **MS 5.10** Dezember 2016: CSIRT BIT ausgebaut, um die Detektionsfähigkeit zu erhöhen.		
M 6	**Konzept Übersicht Straffälle und Koordination interkantonaler Fallkomplexe** Bund und Kantone haben den Weg ihrer künftigen Zusammenarbeit zur Koordination interkantonaler Fallkomplexe in einem Konzept festgehalten, das dem Bundesrat vorgelegt wird. Dieses beschreibt, wie auf nationaler Ebene eine möglichst vollständige Fallübersicht (Straffälle) geführt werden soll, und gibt so auch Auskunft über die Ausgestaltung der Schnittstellen mit weiteren Akteuren auf dem Gebiet der Minimierung von Cyber-Risiken und über die Prozesse des Informationsflusses für die Lagedarstellung. Die Koordination interkantonaler Fallkomplexe ist mit den bereits bestehenden internationalen Bestrebungen zur strafrechtlichen Verfolgung von Cyber-Risiken abzustimmen. Auch weist das Konzept aus, ob auf Stufe Bund und Kantone rechtliche Grundlagen anzupassen und Ressourcen für die Umsetzung des Konzepts bereitzustellen sind. Informationen aus der Fallübersicht (Straffälle) und Erkenntnisse zu Fallkomplexen aus der technisch-operativen Analyse der Strafverfolgung in Strafverfahren werden fortlaufend an MELANI weitergegeben. Im Gegenzug lässt MELANI KOBIK strafrechtsrelevante Informationen aus ihren Erkenntnissen (CERT- und ND-Informationen) fortlaufend zukommen. Hierfür sind bundesinterne und -externe Prozesse etabliert.	**MS 6.1** September 2013: Arbeitsgruppe 4 und Projektorganisation fedpol sind zusammengestellt. **MS 6.2** Juni 2014: erste Vernehmlassung des Konzepts ist abgeschlossen. **MS 6.3** Dezember 2014: zweite Vernehmlassung des Konzepts ist abgeschlossen. **MS 6.4** September 2015: Konzept ist durch KKJPD gutgeheissen. **MS 6.5** Dezember 2015: Ämterkonsultation ist durchgeführt. **MS 6.6** Dezember 2016: Vorbereitung zur Realisierung des Konzepts sind abgeschlossen.	**KOBIK;** MELANI, KKM SVS	C) und Cybersecurity Strategy of the European Union

Mass-nah-men	**Ziele**	**Meilensteine**	**Federführung** und Partner	**Abstimmung mit:** A) Risikopolitik des Bundes B) SKI-Strategie C) Strategie Informations-gesellschaft
M 7	**Übersicht Kompetenzbildungsangebote** Wirtschaft, Verwaltung und Zivilgesellschaft können sich bedürfnisgerecht über qualitativ hochstehende Kompetenzbildungsangebote zum Umgang mit Cyber-Risiken informieren. Angebotslücken sind identifiziert und dienen als Grundlage zur Umsetzung der Massnahme 8.	**MS 7.1** Dezember 2013: Übersicht Kompetenzbildungsangebote ist erstellt. **MS 7.2** März 2014: Qualitativ hochstehende Kompetenzbildungsangebote sind als Best Practice Beispiele identifiziert. **MS 7.3** Juni 2014: Best Practice Beispiele der Kompetenzbildungsangebote sind veröffentlicht. Angebotslücken sind erkannt.	**KS NCS;** BAKOM, EDA, BSV	C)
M 8	**Vermehrte Nutzung der Kompetenzbildungsangebote und Schliessung von Angebotslücken** Der Bund hat in Abstimmung mit den Kantonen und der Wirtschaft in einem Umsetzungskonzept festgehalten, wie er eine vermehrte Nutzung der Kompetenzbildungsangebote zum Umgang mit Cyber-Risiken erreichen will. Weiter zeigt das Konzept auf, wie Angebotslücken geschlossen und welche neuen Kompetenzbildungsangebote geschaffen werden sollen.	*Meilensteine werden bis Juni 2014 definiert, da M8 auf den Ergebnissen von M7 basiert.*	**KS NCS;** BAKOM, EDA, BSV	C)

Mass-nah-men	**Ziele**	**Meilensteine**	**Federführung** und Partner	**Abstimmung mit:** A) Risikopolitik des Bundes B) SKI-Strategie C) Strategie Informations-gesellschaft
M 9	**Internet Governance** Die Interessen von Behörden, Wirtschaft und Gesellschaft der Schweiz betreffend des Themas Internet Governance sind koordiniert. Dazu wurden entsprechende Prozesse definiert. Die vom UVEK betriebene Multistakeholder-Austausch-Plattform wird von den relevanten Akteuren zur Diskussion von Internet Governance-Themen benutzt. Die Interessen der Schweiz im Bereich Internet Governance werden in entsprechenden internationalen Gremien und Veranstaltungen vertreten und die Kooperation mit Partnern auf internationaler Ebene ist sichergestellt.	**MS 9.1** Dezember 2013: Übersicht zu prioritären Veranstaltungen, Initiativen und internationalen Gremien mit Bezug zur Internet-Governance ist erstellt. **MS 9.2** Juni 2014: Übersicht zu den Prozessen zur Internet Governance und zur Beteiligung der Schweiz ist erstellt. **MS 9.3** Dezember 2014: Prioritäten der Schweiz sind gesetzt, einzubindende Akteure identifiziert und Synergien ausgeschöpft. **MS 9.4** Dezember 2015: Ergebnis der Analyse der Wirkung der in M9 definierten Prozesse und eingesetzten Akteure liegt vor.	**BAKOM**; EDA, SIPOL, MELANI, Fachbehörden/ Regulatoren	C)
M 10	**Internationale Kooperation Cyber-Sicherheit** Die Interessen von Wirtschaft, Gesellschaft und Behörden sind auf der Ebene der internationalen Sicherheitspolitik bezüglich Cyber-Risiken koordiniert. Internationale Kooperation, um der Bedrohung im Cyber-Raum in Zusammenarbeit mit anderen Staaten und internationale Organisationen zu begegnen, sind sichergestellt.	**MS 10.1** Dezember 2013: Konzept zur NCS-Umsetzung in internationaler Zusammenarbeit ist erarbeitet. **MS 10.2** Dezember 2014: Fachgruppe Cyber International (FG-CI) ist operativ. **MS 10.3** Dezember 2017: Gezielte Aktivitäten der internationalen Zusammenarbeit gegen Bedrohungen im Cyber-Raum sind im Gange. Möglichkeiten des Einsatzes von internationalen Instrumenten werden geprüft.	**EDA;** SIPOL, MELANI, BAKOM	

Mass-nah-men	Ziele	Meilensteine	Federführung und Partner	Abstimmung mit: A) Risikopolitik des Bundes B) SKI-Strategie C) Strategie Informations-gesellschaft
M 11	**Internationale Initiativen und Standardisierungsprozesse im Bereich Sicherheit** Die Interessen des Wirtschaftsstandortes Schweiz werden koordiniert in die internationalen privaten und staatlichen Gremien im Bereich Sicherheit, Sicherung und Standardisierung eingebracht. Dazu wurde der Informationsaustausch zwischen KI-Betreibern, IKT-Leistungserbringern, Systemlieferanten, Verbänden, nationalen Standardisierungsorganisationen, Fachbehörden und Regulatoren gestärkt. Ein diesbezüglicher Prozess ist etabliert.	**MS 11.1** März 2014: Übersicht zu internationalen Initiativen, Konferenzen und weiteren Gremien im Bereich Sicherheit, Sicherung und Standardisierung. **MS 11.2** Dezember 2014: Übersicht zu den beteiligten Akteure der Schweiz und ihrer Tätigkeiten ist erstellt (Anwender und Normenschaffende). **MS 11.3** Dezember 2015: Prioritäre Wirkungsbereiche für den Wirtschaftsstandort Schweiz sind gesetzt, einzubindende Akteure identifiziert. Mit diesen Akteuren ist ein geeigneter Prozess zum Informationsaustausch definiert. **MS 11.4** Dezember 2016: Ergebnis einer Analyse der Wirkung der in M11 definierten Prozesse und eingesetzten Akteure liegt vor.	**BAKOM;** Fachbehörden/ Regulatoren, EDA, MELANI	
M 12	**Kontinuitätsmanagement** In den 28 kritischen Teilsektoren[2] sind in Zusammenarbeit mit den entsprechenden Fachbehörden und Verbänden die Ergebnisse der Risiko- und Verwundbarkeitsanalysen in entsprechende Kontinuitäts- und Krisenmanagementpläne umgesetzt. Sektor spezifische Gesetzgebungen wurden bedarfsgerecht angepasst. Der freiwillige Informationsaustausch von KI-Betreibern, IKT-Leistungserbringern und Systemlieferanten wird von MELANI unterstützt, um die Kontinuität und Widerstandsfähigkeit auf der Basis der Selbsthilfe zu stärken. Die forensischen Fähigkeiten von MELANI wurden dazu ausgebaut.	*Meilensteine werden bis September 2015 definiert, da M12 auf den Ergebnissen von M2 basiert.*	**BWL, BABS; Fachbehörden/ Regulatoren**; MELANI	A) und B)

[2] s. FN 1.

Mass-nah-men	Ziele	Meilensteine	Federführung und Partner	Abstimmung mit: A) Risikopolitik des Bundes B) SKI-Strategie C) Strategie Informations-gesellschaft
M 13	**Krisenmanagement** In den 28 kritischen Teilsektoren[3] sind in Zusammenarbeit mit den entsprechenden Fachbehörden und Verbänden die Ergebnisse der Risiko- und Verwundbarkeitsanalysen in entsprechende Krisenmanagementpläne umgesetzt. Sektor spezifische Gesetzgebungen wurden bedarfsgerecht angepasst. Die betroffenen Akteure werden in einer Krise durch MELANI subsidiär unterstützt mit der Bereitstellung von Expertenwissen. Der freiwillige Informationsaustausch mit KI-Betreibern und internationalen Partnern wird sichergestellt sowie der adäquate Einbezug polizeilicher Stellen. Die forensischen Fähigkeiten von MELANI wurden dazu ausgebaut. Mittels einer systematischen Zusammenarbeit mit relevanten IKT-Leistungserbringern und Systemlieferanten wurden zusätzliche Fähigkeiten und Kapazitäten geschaffen, um eine Krise zu bewältigen. Das EDA wird informiert bei Fällen mit möglichen aussenpolitischen Implikationen und ist eingebunden bei der Erarbeitung von entsprechenden Vorsorgeplanungen.	*Meilensteine werden bis September 2015 definiert, da M13 auf den Ergebnissen von M2 basiert.*	**BWL, MELANI, BABS;** KOBIK, EDA, Fachbehörden/ Regulatoren	A) und B)

[3] s. FN 1.

Mass-nah-men	Ziele	Meilensteine	Federführung und Partner	Abstimmung mit: A) Risikopolitik des Bundes B) SKI-Strategie C) Strategie Informations-gesellschaft
M 14	**Aktive Massnahmen und Identifikation der Täterschaft** Im Falle einer spezifischen Bedrohung Zusammenhang mit Cyber-Risiken verfügt der NDB, in Kooperation mit ausländischen Partnern, über die Fähigkeit zur Identifikation der Täterschaft. Dies mit Unterstützung von FUB und MND als Leistungserbringer. Die Bundesanwaltschaft erhält vom NDB, soweit rechtlich zulässig, Erkenntnisse über die Täterschaft. Wenn kein Strafverfahren eingeleitet wird, werden vom NDB aktive Gegenmassnahmen vorbereitet, sofern dazu entsprechende Rechtsgrundlagen (NDG) geschaffen worden sind.	**MS 14.1** Dezember 2013: Cyberaspekte des Auftrags NDB sind identifiziert und die Organisationsstruktur ist definiert. **MS 14.2** März 2014: Service Level Agreement (SLA) zusammen mit FUB-ZEO ist angepasst. **MS 14.3** Dezember 2015: Spezialwissen bei NDB mit FUB-ZEO und MND als Leistungserbringer ist aufgebaut.	**NDB, MELANI;** KOBIK, FUB; MND	
M 15	**Konzept für Führungsabläufe und –prozesse mit Cyber-Ausprägung** Ein Konzept für Führungsabläufe und -prozesse zur zeitgerechten Problemlösung, das der Cyber-Ausprägung Rechnung trägt, ist erstellt. Ebenso ist das allgemeine Krisenmanagement, unter Einbezug der zuständigen Partner in Sachen Cyber-Risiken angepasst und beinhaltet den Cyber-Aspekt.	**MS 15.1** November 2013: Konzeptentwurf für Führungsabläufe und –prozesse liegt vor. **MS 15.2** Dezember 2013: Konzept für Führungsabläufe und –prozesse, das den Cyber-Ausprägungen Rechnung trägt, ist erstellt.	**BK**	B)
M 16	**Handlungsbedarf rechtliche Grundlagen** Die zuständigen Departemente haben bestehende Gesetzgebungslücken als prioritär identifiziert und die nötigen rechtlichen Anpassungen gemacht und die dazu nötigen Entwürfe auf den passenden Normstufen erarbeitet. Ein Regelungskonzept wird dem Bundesrat vorgelegt.	**MS 16.1** Dezember 2013: Erste Übersicht zum vordringlichen Gesetzgebungs- und Revisionsbedarf im Cyber Bereich ist erarbeitet. **MS 16.2** September 2014: Regelungskonzept mit Zeitplanung für die als prioritär identifizierten Gesetzgebungslücken liegt vor. **MS 16.3** Dezember 2014: Regelungskonzept ist dem Bundesrat vorgelegt.	**KS NCS**	B)