Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Wirtschaft, Bildung und Forschung WBF

Staatssekretaariat für Wirtschaft SECO
Schweizerische Akkreditierungsstelle SAS

Besprechungsergebnis

Art der Besprechung:	Arbeitssitzung Sektorkomitee Informationstechnologie
Datum:	Freitag, 23.06.2017
Ort:	SECO, Holzikofenweg 36, 3003 Bern, Raum HO36-1.019
Zeit:	09:30 – 15:00h
Vorsitz:	Herr Thomas Hilger SAS
Protokoll:	Herr Thomas Hilger SAS

Anwesend:

Herr Christian Jenny, Bund, BAKOM
Herr Michael von Niederhäusern, Bund, BIT
Herr Peter Stadlin, Fachexperte
Frau Liliane Mollet, insecor, Fachexpertin
Herr Thomas Schmitt, Fachexperte, get it services GmbH
Herr Lorenz Neher, Fachexperte, PWC
Herr Dr. Reinhard Dietrich, SwissSign AG
Herr Clemens Hüppe, KPMG
Herr Pascal Leu, QuoVadis
Herr Hans-Peter Waldegger, Swisscom
Herr Peter Weiss, Swiss Re
Herr Joseph Doekbrijder, S.W.I.S. Group
Frau Raja Chaieb, SQS
Herr Thomas Hilger, SAS
Herr Stephan Gehrke, SAS

Entschuldigt:

Frau Cornelia Enke, SwissSign AG
Herr Peter Bitterli, BDO, Fachexperte
Herr Martin Lechmann, Swisscom
Herr Christoph Graf, SwissSign
Herr Dr. Hans Walter Kramer, Bund, BIT
Herr Andreas Zürcher, Bund, BIT
Herr Thomas Moretti, QuoVadis
Herr Daniel Muster
Herr Patrick Kos, Hoffmann-La Roche
Herr Reto Grubenmann, KPMG
Herr Hans Halstrick, SwissTS

Verteiler:

Mitglieder Sektorkomitee
Leiter Ressort Metrologie und Ingenieurwesen

Traktanden	Ergebnis/Entscheid
1. Begrüssung, Vorstellung und Traktanden Teil 1: ISO-Themen	Traktanden wurden genehmigt
2. Genehmigung Protokolls vom 02.12.2015	Das Protokoll wurde ohne Änderungen angenommen.
3. **Internationale Entwicklung ISMS** (Peter Weiss) - Informationen und Neuigkeiten zur Standardisierung - ISO/IEC 27006:2015	Peter Weiss präsentiert die aktuelle Entwicklung der ISO-Normung auf diesem Gebiet. Die wichtigsten Informationen: - ISO/IEC 27003:2017 (Guidance) ist nun publiziert und die Anwendung bei der Umsetzung der 27001 wird sehr empfohlen - TR 27015 (financial services) wird zurückgezogen - ISO/IEC 27005 (risk management) ist in Überarbeitung, Elemente der ISO 31000 werden berücksichtigt - ISO/IEC 27021 (ISMS professionals) wird 2017 erwartet - 27103 (Cybersecurity) wird bald als TR publiziert werden. ISO27006:2015: Die an die ISO/IEC17021-1:2015 angepasste ISO/IEC27006:2015 wurde am 1. Oktober 2015 publiziert. Die IAF hat eine zweijährige Übergangsfrist festgelegt, am 30. September 2017 endet. Eine Zertifizierungsstelle ist bereits umgestellt, zwei werden in Kürze folgen. Annex B (Auditzeitberechnung) ist nun mandatory.
4. **ISMS Begutachtungspraxis** (Thomas Hilger)	Die neuen Normen ISO/IEC 17021-1:2015 und 27006:2015 stellen für Zertifizierungsstellen teilweise eine grosse Herausforderung dar. Kritische Punkt, die während der Begutachtungen immer wieder ein Thema sind: - Kompetenzanforderungen an die Auditoren und das weitere Zertifizierungspersonal ist nicht einfach bereitzustellen. - Der Scope der Zertifizierung wird oft zu wenig auditiert. - Ebenso SOA und risk assessment/treatment - Klassische QMS/EMS Zertifizierungsstellen haben Mühe bei der Auditierung der technischen Controls. - Die Vereinheitlichung der Auditzeitberechnung hilft die Qualität und Vergleichbarkeit von Audits zu fördern. - Annexe der ISO/IEC27006 sind hilfreich und wirken unterstützend, werden allerdings zu wenig in der Praxis berücksichtigt.
5. kurze Pause	
6. **IT Service Management, ITSM** (Thomas Schmitt) - Neuigkeiten - ITIL - IAF ISO 20000 (MD X)	Thomas Schmitt gibt einen Überblick über die Situation der ISO/IEC 20000-1 sowie ITIL Landschaft in der Schweiz. Im Augenblick sind 9 Standards der 20000-x Reihe publiziert. Nur der -1 enthält Anforderungen. Die anderen sind Guidance Dokumente zur Unterstützung der Implementierung und Anwendung. ISO/IEC20000-6: Diese Norm ist zurzeit im Endstadium der Entwicklung und wird analog zur ISO/IEC 27006:2015 Zusatzanforderungen an akkreditierte Zertifizierungsstellen enthalten, die von der SAS begutachtet werden müssen. Die Publikation wird in Kürze erwartet. Nach Inkrafttreten dieser Norm wird die IAF eine Übergangsfrist bestimmen und das IAF MD18 zurückziehen.
7. **Informationen Zertifizie-**	Der Technische Leiter Zertifizierung berichtet über allgemeine Aktivitäten

Traktanden	Ergebnis/Entscheid
rung allgemein (Stephan Gehrke)	der EA im IAF im Bereich der Zertifizierung. Berührungspunkte sind evtl. die Entwicklungen der IAF im Bereich der mandatory documents MD5 (Audit time for QMS and EMS) und MD11 (audits of integrated management systems).
8. Themenvorschläge für die nächste(n) Sitzung(en)	__
9. Mittagessen	
10. Begrüssung, Vorstellung, Traktanden zum zweiten Teil der Sitzung „Themen betreffend PKI“ Genehmigung Protokoll der Sitzung vom 02.12.2015	Die Traktanden wurden genehmigt Das Protokoll von der letzten Sitzung vom 02.12.2015 wurde ohne Änderung genehmigt.
11. **Informationen e-ID** (Markus Waldner – Fedpol)	Das Konzept für die e-ID ist zurzeit im EJPD zur Ausarbeitung. Es wird damit gerechnet, dass das e-ID Gesetz 2020 in Kraft treten kann. Die geplanten Sicherheitsniveaus sollen es ermöglichen mit der europäischen eIDAS kompatibel zu sein, um eine spätere Notifizierung zu ermöglichen. Die e-ID Anbieter und ihre Systeme müssen durch eine Anerkennungsstelle (VE Bund) anerkannt sein. Die Akkreditierung wird hierbei vermutlich keine Rolle spielen.
12. **Informationen PKI / ZertES** (Christian Jenny) - Aktueller Stand - Neuerungen/Änderungen - Umsetzung	Die Totalrevision über die ZertES ist abgeschlossen und die revidierten Regelungen der ZertES, VZertES und Verordnung des BAKOM (TAV) am 01.01.2017 in Kraft getreten. Wichtigste Änderungen waren: - Einführung des geregelten Zertifikates - Zeitstempel für qualifizierte Signatur, welche der eigenehändigen Unterschrift gleichgestellt ist - Mögl. Einsatz von audiovisueller Kommunikation in Echtzeit zur Personenidentifikation. Bezüglich Anerkennung der Signaturen in der EU gibt es keine Veränderungen.
13. Diverses - Verschiedenes - Themenvorschläge	Gewünschte Themen wären: Risk Assessment (P. Stadlin) ETSI Standardentwicklung und –implementierung, Validator, Signaturinterpretation, auch europ. Interpretation (R. Dietrich),
9. Ort und Datum nächste Sitzung	Für den Bereich PKI wird gewünscht, dass die Sitzungen halbjährlich organisiert werden. Nächste Sitzung wird Q4/2017 gewünscht (doodle-Umfrage) im SECO, Holzikofenweg 36, 3003 Bern

Bern, 08.09.2017 /hit