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:	Mittwoch, 18.12.2013
Ort:	SECO, Holzikofenweg 36, 3003 Bern/Raum 2.238
Zeit:	09:30 bis 12:30 Uhr
Vorsitz:	Herr Thomas Hilger SAS
Protokoll:	Herr Thomas Hilger SAS
Anwesend:	Frau Cornelia Enke, SwissSign AG Herr Joseph Doekbrijder, Swisgroup Herr Christian Jenny, Bund, BAKOM Herr Dr. Rolf Oppliger, Bund, ISB Herr Dr. Reinhard Dietrich, SwissSign AG Herr Thomas Schmitt, USU Consulting Herr Peter Stadlin, Fachexperte Herr Pierre-Yves Baumann, Bund, EDÖB Herr Peter Weiss, Swiss Re Herr Urs Würgler, KPMG Herr Lorenz Neher, Crypto AG, Fachexperte Herr P. Bitterli, Bitterli-Consulting, Fachexperte Herr Erwin Peter, Auditor SQS Herr Carl Rosenast, QuoVadis Herr Michael von Niederhäusern, Bund, BIT Herr Thomas Hilger, SAS
Entschuldigt:	Herr Michael Doujak, SwissSign Herr Reto Grubenmann, KPMG Herr Roman Haltinner Frau Liliane Mollet, Fachexpertin Herr Markus Limacher, Swisscom Herr Hans-Peter Waldegger, Swisscom Herr Christoph Graf, SwissSign Herr Hans Ruedi Münger, Siemens Herr Dr. Hans Walter Kramer, Bund, BIT Herr Daniel Muster Herr Martin Wyss, Auditor SQS Herr Patrick Kos, Hoffmann-La Roche
Verteiler:	Mitglieder Sektorkomitee Leiter SAS Leiter Ressort Metrologie und Ingenieurwesen

Traktanden	Ergebnis/Entscheid
1. Begrüssung, Vorstellung und Traktanden	Traktanden wurden genehmigt
2. Genehmigung Protokolls vom 18.12.2012	Das Protokoll wurde ohne Änderungen angenommen.
3**. Internationale Entwicklung ISMS** - Informationen Standardisierung - IAF ISO 27001 - ISO 27006 / ISO17021 - Kalkulationsanleitung	ISO/IEC27001:2013: Die überarbeitete Norm wurde am 1. Oktober 2013 publiziert. Sie ist neu strukturiert und enthält eine zeitgemässe Sprache. Der PDCA Kreis wurde herausgenommen, was nicht bedeutet, dass ein Managementsystem nicht mehr der kontinuierlichen Verbesserung genügen muss. Die Guidance Documents ISO27003/4/5 bekommen ein höheres Gewicht. Ebenso muss das Risiko nicht nur auch auf das Informationssicherheitssystem, welches durch das ISMS gemanagt wird, bezogen werden, sondern auch auf das ISMS System selbst. Es gibt ein frei zugängliches Mapping Dokument unter: http://www.jtc1sc27.din.de/sbe/wg1sd3 ISO/IEC27002:2013: In der neue Norm wurden die Control Areas neu strukturiert und wo möglich zusammengefasst. Die überarbeitete Version enthält neu 35 statt 39 Control Areas und 114 statt 133 Controls. ISO27006:2011: Die Umstellung von der Version 2007 auf die neue Norm musste gem. IAF ID5 am 31.05.2013 abgeschlossen sein. Die SAS konnte 3 von 4 Zertifizierungsstellen die Konformität zum Stichtag bestätigen. Die Arbeiten zur „grossen" Revision der Norm wurden angegangen. Unter anderem soll die Methodik zur Bestimmung der Auditzeiten überarbeitet werden. Die Schweiz hat die Möglichkeit Vorschläge einzubringen. Es wird ein Subkomitee bestehend aus den Herren Weiss, Stadlin, Peter, Grubenmann und Hilger gebildet, welches sich dieser Aufgabe annehmen wird. Diese Gruppe wird das Dok. 521 (Annex D) überarbeiten und die Kalkulationsanleitung soll fertiggestellt und als Best Practice publiziert werden. Die ISO SC27 hat eine Study Group für das Framework PKI ins Leben gerufen. Es werden noch Mitglieder und Experten für dieses Subcommittee gesucht. Umstellung der ISO/IEC27001:2013: Gemäss IAF Resolution 2013-13 von Oktober 2013 ist eine zweijährige Übergangsfrist vorgesehen, d.h. alle Zertifikate im Feld müssen bis zum 1. Oktober 2015 ausgetauscht werden. Ab dem 1.Oktober 2014 dürfen nur noch Zertifikate nach der neuen ISO/IEC27001:2013 ausgestellt werde. Die SAS wird die betroffenen Zertifizierungsstellen schriftlich über die geplante Vorgehensweise informieren. Die SQS merkt an, dass für die Umstellung bei den Kunden der Zeitrahmen und Umfang eines Re-Zertifizierungsaudit nötig ist. Aus diesem Grund wird angefragt, ob die SAS die Frist auf 3 Jahre ausdehnen kann, damit die Umstellung während der regulär geplanten Re-Zertifizierungsaudits stattfinden kann. Die SAS wird dies abklären. (Nachtrag vom 15.01.2014: Der Antrag auf Verlängerung der Übergangsfrist auf 3 Jahre wurde während der IAF Generalversammlung in Korea gestellt und diskutiert, allerdings wurde dieser Antrag abgelehnt und die kommunizierte 2-Jahresfrist beschlossen. Die SAS hat als Mitglied der IAF keine Möglichkeit von dieser

Traktanden	Ergebnis/Entscheid
	Resolution abzuweichen).
4. **IT Service Management, ITSM** - Pläne der AG SC 40 - Neuer Besitzer ITIL - IAF ISO 20000 (WD 7)	SC40: Die für die ISO 20000-1 zuständige Arbeitsgruppe JTC1 hat ein Subcommittee SC40 gegründet zuständig für das Arbeitsgebiet IT Service Management and IT Governance mit dem Ziel Normen, Guidelines, Best Practices und verwandte Dokumente zu entwickeln. In das Aufgabengebiet fällt ebenso die Entwicklung der ISO/IEC 38500 Normenserie. ITIL: Neuer Besitzer ITIL ist die Axelos, ein Joint Venture der britischen Regierungsbehörde Cabinet Office mit der auf Outsourcing spezialisierten Capita PLC. Durch den Wechsel soll der britische Steuerzahler entlastet werden, ebenso erhofft man sich einen professionelleren Service. Die neue Ausrichtung wird wohl marktorientierter sein, was gewisse Services in Zukunft kostenpflichtig macht. Ebenso wird erwartet, dass die ATOs (accredited training organisations) höhere Hürden zu überwinden haben. IAF ISO20000-1 WD7: Eine Arbeitsgruppe der IAF arbeitet an einem Mandatory Document MD x.y, welches als WD 7 vorliegt. Das Ziel des Dokumentes soll es sein, die Anwendung der ISO/IEC 17021:2011 im Bereich ITSM zu definieren. Da dieses Dokument allerdings keine über die ISO/IEC 17021:2011 hinausgehenden Regelungen enthält und die dort aufgeführten Präzisierungen „offensichtlich“ sind, wird beschlossen, dass dieses Dokument abzulehnen sei.
5. Pause	
6. **Informationen PKI / Qualifizierte Zertifikate** - Totalrevision des Bundesgesetzes vom 19.12.2003 über Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES)	Eine Revision des Bundesgesetzes vom 19. Dez. 2003 über Zertifizierungsdienste im Bereich der elektronischen Signatur ist in Arbeit. Mit dieser Totalrevision des ZertES sollen weitere Anwendungen von elektronischen Zertifikaten geregelt werden. Nebst der bisherigen qualifizierten elektronischen Signatur für natürlichen Personen, möchte man 2 weitere Signaturen regeln: -die geregelte elektronische Signatur mit etwas reduzierten Anforderungen -das geregelte elektronische Siegel, welches auch juristischen Personen und Behörden zugänglich ist. Als weitere Anwendung elektronischer Zertifikate soll auch die sichere Authentifizierung gesetzlich geregelt werden. Wo immer möglich, soll der Einbezug der elektronischen Signatur oder des elektronischen Siegels in den verschiedenen Gesetzen und Verordnungen terminologisch bereinigt bzw. vereinfacht werden. Der Zeitstempel wird zwar nicht für die qualifizierte elektronische Signatur gemäss ZertES vorgeschrieben, jedoch für die Anerkennung dieser Signatur im OR als Ersatz für die eigenhändige Unterschrift. Zeitlicher Ablauf: Die Vernehmlassung wurde durchgeführt und das EJPD hat die Botschaft erarbeitet. Ergebnisse des Vernehmlassungsverfahrens finden sich auf der Vernehmlassungs-Website der Bundeskanzlei (http://www.admin.ch/ch/d/gg/pc/ind2012.html). Es wird damit gerechnet, dass der Bundesrat das Geschäft im Januar 2014 behandelt und anschliessend an das Parlament übergibt. Im Jahr 2014 soll in der EU die neue Verordnung zur elektronischen Signatur verabschiedet werden (Anmerkung: eine Verordnung gilt automatisch in allen Mitgliedstaaten). Eine gegenseitige Anerkennung der Verordnungen EU-CH ist vorgesehen.

Traktanden	Ergebnis/Entscheid
7. **Informationen Daten-schutz** - keine Informationen	Keine Informationen
8. Themenvorschläge für die nächste Sitzung	Bezüglich der Änderungen im Bereich PKI wird angeregt Herrn Urs Paul Holenstein (BJ) in das SK einzuladen.
9. Ort und Datum nächste Sitzung(en)	3. Dezember 2014
10. Diverses	---

Bern-Wabern, 15.01.2014 /hit