Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidg. Volkswirtschaftsdepartement EVD
Staatssekretaariat für Wirtschaft SECO
Schweizerische Akkreditierungsstelle SAS

Besprechungsergebnis

Art der Besprechung:	Arbeitssitzung Sektorkomitee Informatiksicherheit (ITS)
Datum:	Dienstag, 18.12.2012
Ort:	SAS, Lindenweg 50, 3003 Bern-Wabern/Raum HB20
Zeit:	09:30 bis 12:30 Uhr
Vorsitz:	Herr Thomas Hilger SAS
Protokoll:	Herr Thomas Hilger SAS
Anwesend:	Herr Reto Grubenmann, KPMG Herr Roman Haltinner 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 Burkhard Schwalm, Bund, EDÖB Herr Thomas Meier, Bund, EDÖB Herr Michael Doujak, SwissSign Herr Peter Weiss, Swiss Re Herr Thomas Hilger
Entschuldigt:	Frau Liliane Mollet, Fachexpertin Herr Andreas Zürcher, Bund, BIT Herr Markus Limacher, Swisscom Herr Hans-Peter Waldegger, Swisscom Herr Martin Lechmann, Swisscom Herr P. Bitterli, Bitterli-Consulting, Fachexperte Herr Christoph Graf, SwissSign Herr Adrian Humbel, SwissSign Herr Hans Ruedi Münger, Siemens Herr Dr. Hans Walter Kramer, Bund, BIT Herr Peter Keller, Swisscom Herr Roman Brunner, QuoVadis Herr Daniel Muster Herr Wolfgang Schwarz, Auditor SQS Herr Patrick Kos, Hoffmann-La Roche Herr Carl Rosenast, QuoVadis Herr Lorenz Neher, Crypto AG Herr Erwin Peter, Auditor SQS

Verteiler: Mitglieder Sektorkomitee
Leiter SAS
Leiter Ressort Metrologie und Ingenieurwesen

Traktanden	Ergebnis/Entscheid
1. Begrüssung, Vorstellung und Traktanden	Keine neuen Traktanden beantragt
2. Genehmigung Protokolls vom 24.05.2011	Das Protokoll wurde ohne Änderungen angenommen.
3**. Internationale Entwicklung ISMS** - Informationen Standardisierung - IAF ISO 27001 - ISO 27006 / ISO17021 - Kalkulationsanleitung	ISO/IEC27001: Es wird im Herbst 2013 die Publikation der neuen überarbeiteten Version erwartet. Es wurde diskutiert, ob die Anforderungen eher offen formuliert sein sollen (somit hat es Interpretationsspielraum) oder ob wie bisher in Form von Controls beschrieben sein sollen. ISO/IEC27002: Die WG hat gegen 1000 Kommentare erhalten. Es wird eine neue Struktur eingeführt. Controls werden zusammengefasst. Vermutlich gibt es 35 Control Areas und 113 Controls. Risk Assessment und Treatment wurden herausgenommen. Hier kommt die ISO27005 bzw. ISO 31000 zur Anwendung. ISO/IEC27006: Die im Dezember 2011 veröffentlichte Version muss bis Ende Mai 2013 umgesetzt werden (s. IAF ID5). Hierbei handelt es sich um kleinere Anpassungen, um mit der ISO/IEC17021:2011 kompatibel zu sein. Die „grosse" Revision wird im Frühjahr 2014 erwartet. Es wird vorgeschlagen nach dem Erscheinen den Annex D (SAS Dok. 521) anzupassen. Die Kalkulationsanleitung soll fertiggestellt und als Best Practice publiziert werden.
4. IT Service Management, ITSM - ISO 20000-11 (Referenz zu ITIL) - ISO90006 (Service Management) - Überarbeitung Checkliste Dok. 527e - IAF ISO 20000 (WD 6.5) - Follow-up Kalkulationsanleitung für die Budgetierung einer ISO20000-1 Zertifizierung	Nach der ISO 20000-1 Hauptnorm wurde ebenfalls ITIL à jour gebracht. ISO 20000-11 *Guidance on the relationship between ISO/IEC 20000-1:2011 and service management frameworks* enthält ein Mapping ITIL zu ISO 20000-1, ähnlich wie das SAS Dok 527. Aus diesem Grund soll die SAS Checkliste Dok. 527e nicht überarbeitet werden und kann noch beibehalten werden. Die ISO 90006 *Guidelines for the application of ISO 9001:2008 to IT service management and its integration with ISO/IEC 20000-1:2011* soll im Sommer 2013 publiziert werden. Es ist unklar, in welchen Bereichen diese Norm Anwendung finden soll. Eine Arbeitsgruppe der IAF arbeitet an einem Mandatory Document MD x.y, welches als WD 6.5 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 Regelungen enthält, die über die ISO/IEC 17021:2011 hinausgehen, wie z.B. Richtlinien zur Berechnung der Auditzeit oder spezifische Anforderungen an die Auditorenkompetenz, wird die SAS dieses Dokument ablehnen.
4. **Informationen PKI / Qualifizierte Zertifikate** - Neuigkeiten zur Überarbeitung der TAV	Eine Revision des Bundesgesetzes vom 19. Dez. 2003 über Zertifizierungsdienste im Bereich der elektronischen Signatur ist geplant. Zurzeit sind elektronische Unterschriften von juristischen Personen nicht geregelt. Die Entwicklung in Europa soll berücksichtigt werden. Das EJPD wird den Lead übernehmen und die Vorschläge zur Vernehmlassung ausarbeiten.

Traktanden	Ergebnis/Entscheid
6. **Informationen Datenschutz** - Neuigkeiten VDSZ - Datenannahmestelle	Weitere Arbeiten im Bereich der Produktezertifizierung der VDSZ sind vorläufig sistiert. Herr Thomas Meier stellt die Anforderungen im Bereich der Datenannahmestellen von Krankenkassen vor (Art.59a, KVV). Es gibt zwei Datensätze in einem Container (XML 4.3 gemäss Forum Datenaustausch), einen administrativer Datensatz (DRG) und einen medizinischer Datensatz (MCD: Minimal Clinical Dataset). Der medizinische Datensatz unterliegt höheren datenschutzrechtlichen Anforderungen aufgrund der Sensibilität der Daten. Wichtig in diesem Bereich sind die genaue Abgrenzung des Scopes und die Auditoren-kompetenz. Für die Krankenkassen ist eine Zertifizierung nach VDSZ ab 1. Januar 2014 obligatorisch.
8. Themenvorschläge für die nächste Sitzung	Keine
9. Ort und Datum nächste Sitzung(en)	Mai/Juni (Ort noch festzulegen)
10. Diverses	---

Bern-Wabern, 13.12.2013 /hit