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:	Freitag, 29.10.2010
Ort:	SAS, 3003 Bern-Wabern / HB 20 (Neubau, 1. Stock)
Zeit:	09:00 bis 12:30 Uhr
Vorsitz:	Herr Thomas Hilger SAS
Protokoll:	Herr Thomas Hilger

Anwesend:

Pierre-Yves Baumann, Bund, EDÖB
Herr Dr. Rolf Oppliger, Bund, ISB
Herr Christian Jenny, Bund, BAKOM
Herr Peter Stadlin, Fachexperte
Frau Liliane Mollet, Fachexpertin
Herr Markus Limacher, Swisscom
Herr Reto Grubenmann, KPMG
Herr Joseph Doekbrijder, Swisgroup
Herr Thomas Schmitt, get IT Services
Herr Daniel Muster, Bund, Bundeskanzlei
Herr Christoph Graf, SwissSign
Herr Roman Haltinner, KPMG
Herr Reinhard Dietrich, Health Info Net
Herr Hans Ruedi Münger, Siemens
Herr Peter Weiss, Swiss Re
Herr Hans-Peter Waldegger, Swisscom

Entschuldigt:

Herr Dr. Thomas Pimpl, SAS
Herr Peter Keller, Swisscom
Herr Wolfgang Schwarz, Auditor SQS
Herr Erwin Peter, Auditor SQS
Herr Carl Rosenast, QuoVadis
Herr Roman Brunner, QuoVadis
Herr Patrick Kos, Hoffmann-La Roche
Herr P. Bitterli, Bitterli-Consulting, Fachexperte
Herr Michael Doujak, SwissSign
Herr Adrian Humbel, SwissSign
Herr Dr. Hans Walter Kramer, Bund, BIT
Herr Martin Lechmann, Swisscom
Herr Daniel Markwalder, Bund, BIT
Herr Lorenz Neher, Crypto AG
Herr Anthony Thorn, ISSS
Herr Andreas Zürcher, Bund, BIT

Verteiler: Mitglieder Sektorkomitee
Leiter SAS
Leiter Ressort Metrologie und Ingenieurwesen

Traktanden	Ergebnis/Entscheid
1. Begrüssung und Traktanden	Keine Änderungen der Traktanden
2. Genehmigung Protokolls vom 21.05.2010	Erfolgte einstimmig. Es wurde beschlossen die Protokolle der Sitzung zukünftig auf der Internetseite des SK zu veröffentlichen.
3. Aufgaben des Sektorkomitees - Auftrag - Mitglieder	In den letzten Jahren hat sich die personelle Zusammensetzung des SK zum Teil stark geändert. Um ein gemeinsames Verständnis zu erlangen präsentiert Thomas Hilger den Auftrag des SK. (s. Beilage). Die Sitzungsfrequenz von 2 Sitzungen pro Jahr wird von den Teilnehmern begrüsst. Die Zusammensetzung der Teilnehmer ist dem Auftrag angepasst. Es sind alle interessierten Kreise vertreten. Es wird gefragt, ob alle Zertifizierer, die in diesem Bereichen tätig sind, an dieser Sitzung teilnehmen sollten. Da 2 von 3 Zertifizierern Mitglieder sind, ist dies theoretisch ausreichend. Th. Hilger wird die SGS anfragen, ob sie an einer Teilnahme interessiert ist.
5. **ISO 20000-1 ITSM** - Follow up Checkliste als SAS Dokument - Follow up Kalkulationsanleitung für die Budgetierung einer ISO20000-1 Zertifizierung.	Checkliste: Die CL ist soweit fertiggestellt. Ziel ist es, dass die CL den Fachexperten der SAS Hilfestellung bei den Witnessaudits bietet. Ebenso können Zertifizierungsstellen und deren Kunden darauf zugreifen und diese CL als Referenz benutzen. Durch das Mapping zu ITIL und anderen Referenzen ist dies eine einzigartige und vollständige Vorlage geworden. Es liegt ein Schreiben der SQS vor, dass 1.) die Benutzung des Ausdrucks "Controls" irreführend sei, weil die ISO 20'000 nur Anforderungen an ein Managementsystem stelle 2.) die in der Spalte "Conformity Reference" erwähnten BSI Publikationen der Serie "Archieving ISO/IEC20000" (BIP) fälschlicherweise Vorgaben für die Zertifizierung darstellen 3.) die Checkliste mit Hinweisen auf die BIP und ITIL Anforderungscharakter für Audits an Kunden definiert, die nicht nötig sind. Zu 1.) Die Norm redet klar und eindeutig von "Controls" im Sinne von Forderungen. Die sprachliche Erklärung im Vorwort soll aber noch überprüft werden. Zu 2.) Um die Umsetzung der ISO20'000 beim Audit richtig beurteilen zu können, muss der Auditor die BSI-BIP kennen. Das BIP beschreibt die Tätigkeiten sehr genau und detailliert. Auditoren können im BIP nachschauen und müssen nicht interpretieren. Im Punkt 2 der CL "Audit related information" ist der Hilfestellungscharakter beschrieben. Somit werden keine weiteren Anforderungen gestellt. Zu 3.) ISO20'000 und somit die Checkliste verlangt nicht, dass ITIL oder BIP umgesetzt werden. Es hat aber klare Vorteile! Die Arbeitsgruppe wird versuchen alle Definitionen in den einleitenden Kapiteln so eindeutig wie möglich zu gestalten.

Traktanden	Ergebnis/Entscheid
	Herr Schwarz und die SQS bestehen darauf, obwohl sie an der CL mitgearbeitet haben, aus der Autorenliste gestrichen zu werden. Die Checkliste wurde an weitere internationale Organisationen wie ITSMF sowie als Input an IAF, die ein z.Zt. Mandatory Document für die Umsetzung der ISO 20'000 entwickelt, weitergeleitet. <u>Kalkulationsanleitung</u> Die Kalkulationsanleitung wird weiterverfolgt. IAF arbeitet ebenfalls an einem MD (s.o.), die eine Kalkulation der Auditzeit beinhaltet. Die SAS hat die Anleitung als Kommentar der IAF working group zur Verfügung gestellt.
6. **ISO 27001 Zertifizierung** ISO 27001 Kalkulationsanleitung für die Budgetierung einer ISO 27001 Zertifizierung	Vielen Dank auch an diese Arbeitsgruppe. Dieses Dokument soll als Best Practice Model Kunden, Beratern und Zertifizierern Hilfestellung bieten und zur Verfügung gestellt werden. Für eine allfällige Überarbeitung der ISO27006 wird gebeten Informationen an Herrn Weiss zu senden.
7. **ETSI TS 102.042 Standardisierung** (Advanced Zertifikate)	Vertreter der KPMG stellen den Stand und Einsatz der Advanced Zertifikate vor. Es liegt eine schriftliche eingegangene Meinung des BIT vor. Fortgeschrittene Zertifikate sollten geregelt werden, da z.B. der Vererbungsgedanke der SuisseID (fortgeschrittenes erbt Regeln des qualifizierten Zertifikates) rechtlich Grenzen gesetzt sind. Die Definitionen, speziell aus rechtlichen Überlegungen, müssten präzisiert werden.
8. **PKI** Update Stand nicht-qualifizierte Zertifikate	Herr Jenny informiert, dass die Arbeitsgruppe zu den nicht-qualifizierten Zertifikaten vorläufig sistiert wurde. Es sind vorab die rechtlichen Grundlagen zu bestimmen. Herr Stadlin präsentiert die Möglichkeiten von DNSSEC vor. DNSSEC könnte zusätzliche Sicherheit im Bereich der Zertifikate bieten, da Spoof DNS erkannt würden. PKI und SSL werden nachwievor gebraucht.
9. Stand Datenschutzzertifizierungen - Produkte-Zertifizierung (Projektstand)	Die Arbeitsgruppe, die die Rahmenbedingungen für die Zertifizierung von Produkten und Dienstleistungen ausarbeiten sollte, wurde vorerst gestoppt. Die CH will keinen Alleingang.
10. Themenvorschläge für die nächste Sitzung	keine
11. Datum nächste Sitzung(en)	24.05.2011 beim BAKOM in Biel
12. Diverses	--

Bern-Wabern, 10.05.2010 /hit