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, 11.11.11
Ort:	SAS, 3003 Bern-Wabern/Raum HA 34
Zeit:	09:30 bis 12:30 Uhr
Vorsitz:	Herr Thomas Hilger SAS
Protokoll:	Herr Dr. Thomas Pimpl

Anwesend:

Herr Roman Haltinner
Herr Reto Grubenmann, KPMG
Herr Joseph Doekbrijder, Swisgroup
Frau Liliane Mollet, Fachexpertin,
Herr Christian Jenny, Bund, BAKOM
Herr Dr. Rolf Oppliger, Bund, ISB
Herr Carl Rosenast, QuoVadis
Herr Lorenz Neher, Crypto AG
Herr Hans-Peter Waldegger, Swisscom
Herr Dr. Reinhard Dietrich, SwissSign AG
Herr Daniel Markwalder, Bund, BIT
Herr Thomas Schmitt, USU Consulting
Herr Peter Stadlin, Fachexperte
Herr Erwin Peter, Auditor SQS
Herr Thomas Hilger
Herr Dr. Thomas Pimpl, SAS

Entschuldigt:

Pierre-Yves Baumann, Bund, EDÖB
Herr Andreas Zürcher, Bund, BIT
Herr Markus Limacher, Swisscom
Herr Martin Lechmann, Swisscom
Herr Markus Schweizer, USU consulting
Herr P. Bitterli, Bitterli-Consulting, Fachexperte
Herr Christoph Graf, SwissSign
Herr Adrian Humbel, SwissSign
Herr Hans Ruedi Münger, Siemens
Herr Anthony Thorn, ISSS
Herr Robert Dietschi, Bund, BIT
Herr Dr. Hans Walter Kramer, Bund, BIT
Herr Michael Doujak, SwissSign
Herr Peter Keller, Swisscom
Herr Roman Brunner, QuoVadis
Herr Peter Weiss, Swiss Re
Herr Daniel Muster
Herr Wolfgang Schwarz, 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	14 Gäste, 2 SAS Keine neuen Traktanden beantragt
2. Genehmigung Protokolls vom 24.05.2011	Das Protokoll wurde angenommen.
3. **ISO 20000-1 (IT Service Management, ITSM)** - Informationen über Stand/Entwicklung der Norm - Stand Checkliste - Follow up Kalkulationsanleitung für die Budgetierung einer ISO20000-1 Zertifizierung	Herr Schmitt, stellt die ISO 20000er-Gruppe in der ISO-Casco-Arbeitsgruppen vor; kurzer Abriss, „wer kümmert sich um diesen Standard“ WG 25 hat einen Businessplan von 39 Seiten und erstreckt sich über 14 Jahre. Man unterscheidet Short- (1-3 a), Mid- (4-6 a) und Long Term (7-14 a). Harmonisierung zwischen den einzelnen Teilen und zu anderen Normen ist wichtiges Anliegen. Präsentiert wurden die neu überarbeiteten Teile aus 2011 (20000 Teil 1-5) und die für das/die nächsten Jahre anstehenden Teile (20000 Teil 7, 8, 10 und 11) 20000 Teil 11 beschäftigt sich mit der Vernetzung von Teil 1 mit ITIL. 20000 Teil 11 ballot draft erschien plangemäss am 14.10.11; Auszüge wurden vorgestellt die Gegenüberstellung ISO 20000 und ITIL gezeigt. BIP und Auswirkung auf das Audit sind nicht in Teil 11 integriert. Vorschlag für das weitere Vorgehen des SK: BIP-Teil aktualisieren (müsste durch die KPMG geleistet werden). Es wurde kurz diskutiert, welche Auswirkung haben die neuen ISO 20‘000er-Teile auf das Audit (Umfang, Technik, etc.). Idee: Mumbay-Conference (IAF) abwarten, wo die Weichen hinsichtlich weltweiter Harmonisierung gestellt werden sollen. Danach die Teile (Technical control, Visual of System Inspection, BIP_Reference, BIP Chapter) des SAS Dokuments 527e) aktualisieren und das Ergebnis auf der SAS-Homepage aufschalten.
4. **ISO 27001 Zertifizierung** Kalkulationsanleitung für die Budgetierung einer ISO 27001 Zertifizierung im Sinne einer Best Practice - Weiteres Vorgehen und Entscheid	Die Anleitung für die Berechnung der Auditzeiten für ISO 27001 wurde 2011 wegen Zeitmangel nicht weiter vorangetrieben. Herr Stadlin schätzt für die Aktualisierung einen Zeitaufwand von einem vollen Arbeitstag zusammen mit einem Vertreter der Wirtschaft (Herr Weiss von der Swiss Re hat bereits bei Herrn Hilger seine Mitarbeit angeboten). Die Problematik bei der bisherigen Berechnungsgrundlage ist, dass man keinen Bezugspunkt hat, d.h. ein Min.- oder Max-Wert sollte zum Vergleich eingeführt werden, damit auch der Kunde sieht, wann ein Angebot schon mangels zeitlichem Aufwand seriös sein kann. Die Diskussion zeigt, dass man sich uneinig war, ob das Dokument weiter bearbeitet werden soll, da es für die im SK mitarbeitenden ZS einen grossen Aufwand bedeutet und der Nutzen fraglich ist. Das Dokument wäre sicher für den Kunden der ZS ein Fixpunkt, der diesem einen Anhaltspunkt geben kann, was für ein seriöses Audit aufgewendet werden muss.

Traktanden	Ergebnis/Entscheid
	Allgemein gilt auch im Bereich der ISO 27‘001, dass die Zertifikate vom Kunden möglichst billig eingekauft werden. „Preise sind gut vergleichbar, Qualität hingegen nicht (ohne weiteres)“. Beschluss: Das Dokument wird finalisiert (Ziel: Jan. 2012)
5.	- -
6. **PKI** - Informationen / Neuigkeiten zur Überarbeitung der TAV - Marktanforderungen im Bereich Mobile ID / Mobile PKI (Diskussion)	Herr Jenny stellt kurz die Entwicklung der qualifizierten und nicht qualifizierten Zertifikate vor. Qualifizierte Zertifikate => Dienste werden auf Grund der Entwicklungen in der EU auch von der Schweiz unterstützt. CEN erarbeitet neues Protection Profil, was für Anfang 2012 erwartet wird. Italien hat vorgängig eigene Lösung erarbeitet. In der Schweiz ist nur die Signatur für natürliche Personen geregelt. Bisher fehlt juristische Grundlage. BA f. Justiz hat letzte Woche zu einer Sitzung eingeladen. Anfang 12 wird die Ämterkonsultation erwartet und Ende 12 eine verbindliche Lösung. Anerkennung durch die CAS soll harmonisiert werden. Ausblick: Was passiert im Bereich TAV. Derzeit erarbeiten viele Länder eine neue gesetzliche Lösung, jedoch sind hier Doppelspurigkeiten zu befürchten, was danach einen erheblichen Harmonisierungsbedarf bringen wird, sowohl in der EU als auch EU mit der Schweiz.
7. Diskussion	Kurze Diskussion über Stress- und Penetrationstest. Es gab Stimmen, die das auf Grund der zu steigernden Awareness, befürworten, andere sahen die Gefahr, dass man sich durchs Bestehen in falsche Sicherheit wiegt. Vorgeschriebene Tests sind somit nicht einheitlich positiv oder negativ eingeordnet. Die Frage des Auftrags, der Verantwortung für die Durchführung und der Bezahlung war ein weiterer Punkt, über den wenig Einigkeit bestand.
8. Themenvorschläge für die nächste Sitzung	1.) 27‘005 Risk assessment – wie geht man vor. Als Background-Info 2.) Mobile Payment (Identity Management)
9. Ort und Datum nächste Sitzung(en)	April/Mai (Ort noch festzulegen) In dieser wird entschieden, ob eine Herbstsitzung stattfindet.
10. Diverses	---

Bern-Wabern, 29.11.2011 /hit