Besprechungsergebnis

Sektorkomitee ITS - Gruppe ISO/VDSZ

Datum	04.02.2022	Anwesend	Thomas Hilger (SAS) Stephan Gehrke (SAS) Peter Weiss (SwissRe) Heinrich Bieler (SSC) Philippe Schwab (EDÖB) Fabienne Schlup (EDÖB) Liliane Mollet (FE) Peter Stadlin (FE) Markus Schweizer (FE)
Ort	MS-TEAMS	Entschuldigt	Reto Grubenmann (KPMG) Daniel Badertscher (SQS)
Zeit	13:30 – 16:00h	Protokoll	Th. Hilger
Vorsitz	Thomas Hilger	z.K. an	gsn

Traktandum	**Ergebnis, Entscheid**
Protokoll	Das Protokoll der letzten Sitzung wurde ohne Änderungen genehmigt und kann auf den Webpages der SAS publiziert werden.
ISO/IEC 27000 Serie Weiterentwicklungen Peter Weiss	ISO/IEC **27002**:2022 steht kurz vor der Publikation. Wichtige Änderungen sind: - einfachere Struktur (4 "Themes" mit "Attributes") - neues Control Layout - Integration generischer Controls aus branchenspezifischen Erweiterungen von ISO/IEC 27002:2013, soweit angemessen - Aktualisierung von Controls und Schliessung von Lücken entsprechend dem Fortschritt bei den Best Practices - Begriffe und Definitionen wurden in das Dokument integriert Neu gibt es 37 **organizational** controls, 8 **people** controls, 14 **physical** controls und 34 **technical** controls.
	ISO/IEC **27001**:2022 wird ebenfalls vermutlich in Q2/22 publiziert. Änderungen betreffen eine minimale Überarbeitung zur Anpassung an den aktualisierten Controls in ISO/IEC 27002:2022, Integration der letzten Änderungen und eine kleine Anpassung, bei der sich der Haupttext auf die „Objectives“ bezieht, die nicht mehr in 27002 enthalten sind sowie der Annex A.

Traktandum	Ergebnis, Entscheid
	ISO/IEC 27006-1. Zurzeit im Stadium 2. CD, Publikation vermutlich in 2023. Die Schweizer Experten Arbeitsgruppe bestehend aus dem Sektorkomitee und der SNV TK149 erstellte vom 21. Nov. bis 22. Jan. eine Aktualisierung des Anhangs D, der am 17. Januar als CH-Kommentar zur 2. CD eingereicht wurde. Recht herzlichen Dank an diese AG! Die weltweite Akzeptanz wird sich nun in den Ballots zeigen.
VDSZ – Revision DSG und VDSZ	Das neue Datenschutzgesetz (nDSG) ist geplant im Zeitraum Mitte-Ende 2022 in Kraft zu setzen. Es bezieht sich ausschliesslich auf Daten von natürlichen Personen. Die Aufzählung der besonders schützenswerten Daten wird um genetische und biometrische Daten (sofern diese eine natürliche Person eindeutig identifizieren) erweitert. Neu können nebst den Betreibern von Datenbearbeitungs-systemen oder -programmen neu auch deren Hersteller ihre Systeme, Produkte und Dienstleistungen zertifizieren lassen. Die **nVDSG** ist noch in der Vernehmlassung. Die neue Verordnung (**nVDSZ**) ist noch nicht definitiv. Es ist je eine separate Akkreditierung erforderlich für die Zertifizierung von: a. Datenbearbeitungssystemen (Organisation, Verfahren und Prozesse); b. Produkten (Hardware, Software oder Systeme für automatisierte Datenbearbeitungsverfahren); c. Dienstleistungen. Aus Sicht Akkreditierung können diesen Vorgaben zwei Akkreditierungsnormen zugeordnet werden. Für die Zertifizierung von Datenbearbeitungssystemen die **ISO/IEC 17021-1** (Managementsystem) für Datenbearbeitungssysteme von Organisationen, resp. evtl. Verfahren und **ISO/IEC 17065** für Produkte, Dienstleistungen und Prozesse. Hierbei sollte darauf geachtet werden, dass die Definition für "Prozesse" aus der nVDSZ keine Verwirrung zur Definition der "Prozesse" im Bereich der Akkreditierung/Zertifizierung stiftet, die durch die ISO/IEC Normen vorgegeben werden. Bei der nVDSZ ist die Definition gem. ISO/IEC 27001 gemeint = Satz zusammenhängender und sich gegenseitig beeinflussender Tätigkeiten, der Eingaben in Ergebnisse umwandelt. Weiter basiert in Europa eine mögliche Zertifizierung für die DSGVO auf der ISO/IEC 17065. Dies muss kein Widerspruch sein, da die ISO/IEC 17065 in Abhängigkeit vom vorgegebene Schema auch Anforderungen nach ISO/IEC 17021-1 beinhalten kann.
ISO/IEC 20000-1/ITIL - ITIL, neue Module, Erfahrungen	Markus Schweizer ist neuer Fachexperte bei der SAS für den Bereich ISO/IEC 20000-1. Thomas Schmitt ist seit 2020 pensioniert. Herr Schweizer stellt sich kurz vor. ITIL hat sich über die letzten 30 Jahre exxtrem weiterentwickelt. Seit 2019 qird mit ITIL V4 gearbeitet. 2021 wurde der Eigentümer der ITIL Library (Axelos) von der Organisation Peoplecert (https://www.peoplecert.org) übernommen. Wie wirkt sich die Corona Pandemie auf das ITSM Budget aus? Es kann festgestellt werden, dass über 51 % der befragten Unternehmen aus dem IT- und Technologiebereich ein teils deutliche erhöhtes Budget für 2021 zur Verfügung haben. Auch sind IT Service Themen das wichtigste strategische Thema mit deutlichem Wachstum geworden. Adoption von ITL 4 im Markt (Auszug):

Traktandum	Ergebnis, Entscheid
	- ITIL 4 Foundation ist seit 3 Jahren unter den Top 3 Kursen der Digicomp - Organisationen in der Schweiz beginnen mit Adoption von ITIL 4 Elementen um angehende Entwicklungen im Bereich Agilität (Scrum, SAFe, DevOps) mit dem operativen Bereich verknüpfen zu können - Value Stream Mapping gewinnt auch im IT Betrieb an Popularität Am 28.07.2021 wurde die **ISO/IEC TS 20000-11:2021** *Guidance on the relationship between ISO/IEC 20000-1 and service management frameworks: ITIL®* publiziert. Dieses Dokument enthält Anleitungen zum Verhältnis zwischen der ISO/IEC 20000-1 und dem häufig verwendeten Service-Management-Framework ITIL 4. Es kann von jeder Organisation oder Person verwendet werden, die verstehen möchte, wie ITIL mit ISO/IEC 20000-1 verwendet werden kann.
Neues aus der IAF, EA und SAS	**Transition ISO/IEC 27006 Amd.1:2020** Publikation des Amendements im 03/2020 Änderungen betreffen hauptsächlich folgende Punkte: - Qualifikation der Auditoren (7.2.1.1 d) & neuer Punkt g) - Klarstellung zum Einbezug von Control sets, welche im SOA Anwendung finden können, bez. Darstellung im Zertifikat. - Freigabe Stufe 1 Bericht durch LA möglich (9.3.1.1) - Annex B: Präzisierungen zur Auditzeitberechnung. Geplanter Abschluss der Umstellung: 31.03.2022* **gem. IAF COVID19 Q&A #20 um 6 Monate verlängert* Situation CH: 1 KBS umgestellt, 1 im Prozess, **1 KBS hat noch kein Gesuch für die Umstellung eingereicht**. Nach Ablauf der Frist (s.o.) **erlischt die Akkreditierung** für ISO/IEC 27001 Zertifizierungen ohne weitere Massnahmen! **Übergangsregeln von ISO/IEC 27001:2013 zu ISO/IEC 27001:2022**: The General Assembly of IAF, acting on the recommendation of the Technical Committee, resolved that the Transitional Arrangement for the Revision of ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements shall be **two years** from the last day of the month of publication of the revised standard. **ISO/IEC TS 27006-2:2021** – Requirements for bodies providing audit and certification of information security management systems - Part 2: Privacy information management systems (PIMS) This document specifies requirements and provides guidance for bodies providing audit and certification of a privacy information management system (PIMS) according to ISO/IEC 27701 in combination with ISO/IEC 27001, in addition to the requirements contained within ISO/IEC 27006 and ISO/IEC 27701. It was agreed in the technical committee to ask IAF **for endorsement** of the standard.

Traktandum	Ergebnis, Entscheid
Diverses	--
Nächste Sitzung und themen	Nächste Sitzung ev. noch in diesem Jahr, abhängig von den Themen.

24.02.2022, Th. Hilger SAS