05/2014

UIMCommunic@tion

Stets auf dem Laufenden sein?
www.UIMC.de/Communication

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Nachweisführung der Qualität der Informationssicherheit!?

Umstellung der ISO 27001: UIMCert als DAkkS-akkreditierter Zertifizierer als kompetenter Unterstützer

Die ISO/IEC 27001 wurde novelliert und im September 2013 als neue Version veröffentlicht. Dies hat zur Folge, dass zertifizierte Unternehmen aber auch Instititutionen, die ihr Informationssicherheits-Managementsystem (ISMS) ohne Zertifizierung an der Norm orientiert haben, den Aufbau der IT-Sicherheits-Organisation prüfen müssen, ob diese auch den neuen Anforderungen genügen. Da dies aufgrund kapazitärer und fachlicher Gründe oftmals nicht ohne externe Unterstützung zu erreichen ist, greifen viele Unternehmen auf akkreditierte Zertifizierungsunternehmen zurück.

Eine Zertifizierung gemäß ISO 27001 kann nur noch bis zum 30. September 2014 nach der „alten" Norm erfolgen; ab dem 1.Oktober 2014 muss diese wiederum zwingend nach der ISO 27001:2013 durchgeführt werden. Dies führt dazu, dass in relativ kurzer Zeit das eigene Informationssicherheits-Managementsystem nicht nur dahingehend geprüft werden muss, ob es den neuen Anforderungen entspricht, sondern ggf. auch entsprechende Maßnahmen zur Anpassung erarbeitet, geplant und umgesetzt werden müssen. So wurde z. B. der gesamte Aspekt des Risikomanagements in der neuen Version deutlich hervorgehoben und an verschiedenen Stellen in den einzelnen Phasen betrachtet. Da bei vielen Unternehmen eine Tendenz zum IT-Outsourcing besteht, ist die Ausweitung der Lieferantenbewertung in der novellierten Norm ebenfalls zu beachten .

Als erfahrenes DAkkS-akkreditiertes Zertifizierungsunternehmen für die ISO/IEC 27001unterstützt die UIMCert auf verschiedene Weisen. In einem Voraudit kann beispielsweise die Zertifizierungsfähigkeit geprüft werden, um so den Status quo des ISMS zu ermitteln. Dies wird toolgestützt durchgeführt, so dass sowohl das Audit selbst als auch die Auswertung ausgesprochen effizient umgesetzt werden können. Des Weiteren werden automatisiert etwaige Maßnahmen abgeleitet, an welchen Stellen das Managementsystem noch optimiert werden sollte. Dadurch kann das ISMS sukzessive und zielführend so angepasst werden, dass eine Ausrichtung gemäß der aktualisierten ISO 27001:2013 erreicht wird. Es kann aber auch sofort eine Auditierung gemäß ISO 27001:2013 durchgeführt werden und bei einem Gutbefund ein ISO-27001-Zertifikat ausgestellt werden.

Die für den Erhalt der Normkonformität essentiellen internen Audits können die UIMCert-Auditoren als Fachexperten ebenfalls begleiten oder auch in Eigenregie durchführen. Durch ein Audit mit externer Unterstützung wird ein aussagekräftiges Ergebnis ermittelt, welches nicht durch möglicherweise fehlende Objektivität oder mangelnde Fachkenntnis im Umfeld der „neuen" Norm beeinflusst wird.

Darüber hinaus kann die UIMCert auch umfassend bei der Vorbereitung zu einer (Neu-) Ausrichtung gemäß ISO 27001:2013 untersützen. So können die Mitarbeiter durch qualifizierte Lead-Auditoren zu den Neuerungen der Norm umfassend geschult werden, um neben Kenntnissen über diese Neuerungen auch die Grundlagen für die Ermittlung von Arbeitsaufwänden zur Anpassung zu vermitteln. Hierbei werden auch Tipps gegeben, wie die Arbeiten strukturiert und effizient umgesetzt werden können.

Mehr Pressemitteilungen finden Sie hier: www.UIMC.de/communication

Schon gewusst?

Das Bestellen eines Newsletters sollte im sog. Double-Opt-In-Verfahren stattfinden, indem dem Nutzer nach Eintragung seiner E-Mail-Adresse ein Link zugesendet wird. Erst nach dieser Bestätigung wird die Registrierung aktiv. Dies wird von den Datenschutzaufsichtsbehörden gefordert und wurde durch verschiedene Gerichte schon als erforderlich definiert. Als Beispiel für eine mögliche Umsetzung können Sie sich an unserer Internetseite orientieren:

UIMC.de/Info-Bestellung

Haben Sie Fragen?
UIMC Dr. Vossbein GmbH & Co KG
Nützenberger Straße 119
42115 Wuppertal
Tel.: (02 02) 2 65 74 - 0
Fax: (02 02) 2 65 74 - 19
E-Mail: consultants@uimc.de
Internet: www.UIMC.de

Noch Fragen?
Treten Sie in einen Dialog ein!

UIMCommunic@tion

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Smartphones und Apps: Tipps für die Installation/Nutzung

Auch Smartphones können von Schadsoftware befallen werden. Gleiches gilt für den Download von Programmen/Apps. Daher sollten, ob privat oder dienstlich, verschiedene Maßnahmen ergriffen werden:

1. Es sollten nur Apps aus **offiziellen Quellen** (also Apple Appstore, Google PlayStore oder Windows Phone Store) installiert werden.
2. Hierbei sind folgende Kriterien zu beachten:
   - » Kontrollieren Sie den **Rechteumfang** der Apps (insbesondere auf persönliche Daten) [Ist es für den Einsatzzweck legitim, der App diese Rechte zu gewähren?]
   - » Informieren Sie sich vorab über die **Seriösität** der App und des Herstellers.
   - » Schränken Sie die Rechte der Apps (sofern möglich) weiter ein, so dass keine unberechtigten/**unnötigen Zugriffe** stattfinden können (insbesondere Adressbuch, E-Mails und Kalender) [im iPhone unter „Einstellungen“ > „Datenschutz“].
3. **QR-Codes** (Quick Response Code) sind nur mit Sorgfalt abzufotografieren, da die hinterlegte Internetadresse auch eine Phishing-Attacke oder Schadsoftware enthalten kann.
4. System-**Updates** sollten unverzüglich durchgeführt werden, da sie oftmals auch Sicherheitslücken schließen.
5. Insbesondere für dienstliche Smartphones gilt:
   - » Es sollten **keinerlei Änderungen** an den Sicherheitseinstellungen der Geräte vorgenommen werden.
   - » Gleiches gilt für das Betriebssystem (also iOS, Android oder WindowsPhone). Ein sog. **Jailbreak** oder die Nutzung von Custom-ROMs sollte nicht stattfinden.

Mehr Tipps finden Sie in der nächsten Ausgabe vom UIMCommunic@tion-Info-Brief oder erfahren Sie bei Ihrem Ansprechpartner!

Auszug aus bisher erschienenen Hinweisen/Tipps:
„Sichere Nutzung von E-Mails“ (09/2013)
„Fernwartung durch Dienstleister“ (02/2014)

(Rechts-) sicheres Outsourcing

Innerhalb des Vortrags auf der diesjährigen IT-Trends „Sicherheit“ werden wir am **14.05.2014 in Bochum** sollen neben der Darstellung der Anforderungen im Rahmen des Out-sourcings auch die Schwierigkeiten, Probleme und besonderen Anforderungen darstellen. Ferner sollen Beispiele aus der Praxis angeführt werden, wie diese Vorgaben pragmatisch umgesetzt werden können/sollen. Auch sollen Lösungsansätze erarbeitet werden.

14.05.2014, Bochum

Koordinierte Dienstleister-Audits

Sobald personenbezogene Daten durch einen Dienstleister eingesehen werden können, muss sich der Auftraggeber von der Einhaltung Ordnungsmäßigkeit überzeugen. Die UIMCert kann eine solche Auditierung auch koordinieren, indem weitere Kunden des Dienstleisters angesprochen und von einer gemeinsamen Auditierung überzeugt werden. Dies kann zu umfasssenden Kostenersparnissen führen. Mehr unter

uimcert.de/dienstleisterauditierung

Bitte senden Sie mir neben den angekreuzten Themen weitere Informationen zu:

- ☐ Umstellung der ISO 27001: UIMCert als DAkkS-akkreditierter Zertifizierer als kompetenter Unterstützer
- ☐ Anforderungen an die rechtskonforme Anmeldung an einen Newsletter
- ☐ **Unser Tipp:** Bitte senden Sie mir zukünftig den UIMCommunic@tion-Info-Brief und regelmäßig weitere interessante Informationen per E-Mail zu! Mir ist bekannt, dass ich der künftigen Zusendung jederzeit formlos per E-Mail an communication@uimc.de widersprechen kann.

E-Mail: _____ Unterschrift: _____

per Fax an (0202) 265 74 - 19 oder formlos per Mail an communication@uimc.de