DSP IT Service GmbH, Schaberweg 28b, 61348 Bad Homburg

Whitepaper zum Thema Risiko Management, Information Security und Service Management im IT-Bereich

Umsetzung des IT-Sicherheitsgesetzes

Das „Gesetz für Transparenz und Kontrolle (KonTraG)“ mit der Forderung nach einem unternehmensweiten Risikomanagementsystem unter Einbeziehung des IT-Bereichs ist dort häufig noch immer nicht wirklich angekommen. Im Juli 2015 wurde das IT-Sicherheitsgesetz von der Bundesregierung verabschiedet und beinhaltet die Einführung eines Information-Security-Management-Systems (ISMS) gemäß ISO 27.000 mit weitreichenden Auswirkungen auf alle IT-Abteilungen.

Die Bundesregierung trägt der Abhängigkeit der Grundversorgung der Bevölkerung von IT-Services und der ständig steigenden Gefährdungslage in der Informationsverarbeitung mit der Verabschiedung des IT-Sicherheitsgesetzes Rechnung. Das Gesetz sieht für alle Unternehmen, die gesetzlich festgelegte Schwellwerte überschreiten und den Sektoren Energie, Informationstechnik, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören, die Einhaltung eines Mindestniveaus an IT-Sicherheit, den Nachweis durch Sicherheitsaudits, die Einrichtung und Aufrechterhaltung von Verfahren für die Meldung erheblicher IT-Sicherheitsvorfälle an das BSI sowie das Betreiben einer Kontaktstelle zur Meldung von Vorfällen an das BSI vor.

Faktisch bedeutet eine Umsetzung des IT-Sicherheitsgesetzes für betroffene Unternehmen die Einführung eines Information-Security-Management-Systems (ISMS) gemäß ISO 27.000 mit regelmäßigen externen Audits und Ablieferung eines ISO 27.000-Zertifikats beim BSI im Jahr 2018 (festgelegt wurde der 31.01.2018 – es ist jedoch mit einer Verlängerung der Frist zu rechnen).

Sollte Ihre Organisation nun nicht die im IT-Sicherheitsgesetz definierten Schwellwerte überschreiten und nicht zur Ablieferung eines ISO 27.000-Zertifikats beim BSI verpflichtet sein, macht es dennoch Sinn weiterzulesen, denn wir stellen fest, dass alle unter das IT-Sicherheitsgesetz fallenden Organisationen ihre Zulieferer ebenso zur Einführung eines ISMS verpflichten!

IT-Abteilungen werden zwingend eng einzubinden sein. Risikomanagement ist dabei eine zentrale Anforderung der ISO 27.000. Bereits das Gesetz für Transparenz und Kontrolle (KonTraG) sieht für mittlere und große Unternehmen die Pflicht zur Einführung eines unternehmensweiten Risiko-Management-Systems vor. Jedoch mangelte es bisher an der praktischen Umsetzung mit der Einbeziehung des IT-Bereichs. Aus unserer Beratungspraxis erfahren wir von einer steigenden Zahl an IT-Security-Projekten und die Nachfrage nach geschulten und erfahrenen Beratern und unterstützenden Systemen steigt. Bevor nun IT-Abteilungen in Hektik geraten und neue Projekte initiieren, lohnt sich die Prüfung der Ausgangslage und auf Interdependenzen zum IT-Service-Management-System (ITSM). Denn davon gibt es viele.

Je nach Reifegrad und Ausbaustufe bietet das IT-Service-Management-System (ITSM) eine ideale Grundlage, die gesetzlichen Anforderungen und das ISMS im IT-Bereich zu unterstützen. In einigen Fällen sehen wir, dass IT-Abteilungen für das ISMS im IT-Bereich parallele Organisationen, Prozesse und Systeme aufbauen.

DSP IT Service GmbH **Schaberweg 28b * 61348 Bad Homburg**
Geschäftsführer: Dr. Steffen Scholtze Telefon: 06172-67946-0
Bad Homburg HRB 7841 Telefax: 06172-67946-9

Bankverbindungen:
Postbank Frankfurt * BLZ: 500 100 60 * Konto Nummer: 7535 89-600 IBAN DE75 5001 0060 0753 5896 00, BIC PBNKDEFF
Taunus Sparkasse Bad Homburg * BLZ: 512 500 00 * Kto: 1050478

Ein reifes IT-Service-Management-System (ITSM) gemäß ISO 20.000 stellt jedoch für das IT-Security-Management-System gemäß ISO 27.000 viele geforderte Grundlagen für den IT-Bereich. So sind in dem IT-Katalog alle produzierten IT-Services gelistet, die CMDB beinhaltet alle Produktionsressourcen (CIs) und deren Beziehungen zu IT-Services, Nutzern und wechselseitigen Abhängigkeiten. Die Kern-Prozesse Incident Management, Change Management, Service Request Management und Problem Management sind implementiert und integrierte ITSM-Systeme unterstützen die Organisation und die IT-Geschäftsprozesse.

Übrigens müsste jede IT-Abteilung, die sich mit ITSM und einer Zertifizierung gemäß ISO 20.000 beschäftigt, sich auch mit den darin enthaltenen IT-Prozessen IT-Security-Management und Business-Continuity-Management for IT-Services beschäftigt haben. ISO 20.000 bietet also für den IT-Bereich den weiteren Rahmen als ISO 27.000. Die Implementierung von Prozessen und Systemen für ISO 27.000 im IT-Bereich bedarf häufig nur der Erweiterung des bestehenden ITSM-Systems. Nach der geforderten Risikoanalyse werden die im Katalog gelisteten IT-Services hinsichtlich ihrer Businesskritikalität gekennzeichnet und kategorisiert. Für die businesskritischen IT-Services sind die unterstützenden CIs ebenso zu qualifizieren und zu kennzeichnen. Die bereits etablierten ITSM-Prozesse sind jeweils für die IT-Security-Anforderungen fit zu machen und die ITSM-Systeme anzupassen. Alles in Allem ist der Aufwand dafür überschaubar, vorausgesetzt, man hat seine Hausaufgaben im Bereich ITIL bereits erledigt und ein nach ISO 20.000 zertifizierungsfähiges ITSM-System in den letzten Jahren implementiert oder ist auf dem Weg dazu. Zusätzlich muss das ISMS mit seiner Policy, dem Risikomanagement, den Regelwerken und der Organisation im IT-Bereich implementiert werden.

Nicht zu vergessen ist die Implementierung eines Notfallplans mit regelmäßigen Tests und Genehmigung von Änderungen durch das Change-Management. Auch sind eventuell die vorhandenen ITSM-Systeme um weitere Module - wie zum Beispiel Systeme für das Data Center Infrastructure Management (DCIM) oder Identity und Access Management Systeme (IAM) - zu erweitern und in das vorhandene ITSM-System zu integrieren.

Die Gefahr liegt darin, dass IT-Abteilungen für das ISMS parallele Strukturen, Prozesse und Systeme einführen, die in Konkurrenz zum ITSM-System stehen, anstatt diese zu ergänzen.

Die Folgen wären erheblicher Mehraufwand im IT-Betrieb, doppelte Organisationsstrukturen, doppelte Systeme, überhöhte Kosten und viel Reibung im Tagesbetrieb über die gesamte IT-Organisation hinweg.

Autor: Dr. Steffen Scholtze, Bad Homburg im August 2017

==========

Über die DSP

Die DSP ist der Spezialist für IT-Service-Management- und IT-Security-Management-Systeme und begleitet Mandanten bis zur ISO 20.000 und/oder ISO 27.000-Zertifizierung. Wir liefern integrierte Lösungen namhafter Hersteller, die die IT-Geschäftsprozesse optimal unterstützen und viele wiederkehrende IT-Geschäftsvorfälle automatisiert bearbeiten. Mit unseren modularen Beratungs-produkten und Lösungen stehen Sie in Bezug auf IT-Service- und IT-Security-Management ganz sicher mit beiden Beinen fest auf dem Boden.

DSP IT Service GmbH
Geschäftsführer: Dr. Steffen Scholtze
Bad Homburg HRB 7841

Schaberweg 28b * 61348 Bad Homburg
Telefon: 06172-67946-0
Telefax: 06172-67946-9

Bankverbindungen:
Postbank Frankfurt * BLZ: 500 100 60 * Konto Nummer: 7535 89-600 IBAN DE75 5001 0060 0753 5896 00, BIC PBNKDEFF
Taunus Sparkasse Bad Homburg * BLZ: 512 500 00 * Kto: 1050478

Wir bieten Ihnen z.B. eine Reifegradanalyse des Management-Systems auf der Basis eines Fragenkatalogs. Ferner erfolgt ein IT-Security-Check anhand einer Analyse der Security-Ausgangslage in Ihrer IT-Abteilung. Mit unseren Penetration-Tests decken wir Schwachstellen und Gefahrenpotenziale auf und verhindern unautorisierte Zugriffe auf Ihre Daten und Systeme. Und wenn ein unautorisierter Zugriff erfolgte, dann ermitteln wir im Rahmen eines Forensic Research, wie der Einbruch erfolgte, welche Systeme und Daten betroffen sind, ermitteln den Schadensumfang und geben Hinweise, wie erneute Einbrüche zu verhindern sind.

Mit dem Security GAP Workshop ist ein Abgleich des Ist-Zustands Ihres Security-Management-Systems möglich und wir können so z.B. einen Maßnahmenkatalog zur Verbesserung Ihrer IT-Security erstellen. Mit dem IT-Security-Funktions- und Prozess-Workshop können Sie darüber hinaus z.B. das Design der IT-Security-Organisation oder die individuelle Zielfunktion festlegen. Ein zertifizierter Security-Management-Consultant wird Ihnen dabei mit Rat und Tat zur Seite stehen. Als akkreditiertes Trainingsinstitut des TÜV-Süd, PeopleCert und EXIN bieten wir Ihnen Trainings und Personen-zertifizierungen an. Mit der DSP können Ihre IT-Mitarbeiter das ITIL Foundation Certificate oder das IT Security Foundation Certificate erwerben oder sich zum zertifizierten Security Penetration Tester oder Security Forensic Researcher ausbilden lassen.

Mit den Lösungen der Matrix42 AG und der CA Technologies – ergänzt um zusätzliche DSP-Lösungen – liefern, implementieren, warten und betreiben wir alle für eine Zertifizierung notwendigen Systeme.

Und wenn Sie bereits Matrix42 in Ihrem Betrieb einsetzen, dann bieten wir Ihnen das DSP-Security-Paket an, das aus den folgenden Modulen besteht:

a. DSP Matrix42 Customizing-Paket für das Security Management
b. DSP Identity und Access Management Modul für Matrix42-User

Sprechen Sie mit uns über die Einführung und Zertifizierung Ihres IT-Service-Management-Systems gemäß ISO 20.000 und/oder IT-Security-Management-Systems gemäß ISO 27.000!

DSP IT Service GmbH
Geschäftsführer: Dr. Steffen Scholtze
Bad Homburg HRB 7841

Schaberweg 28b * 61348 Bad Homburg
Telefon: 06172-67946-0
Telefax: 06172-67946-9

Bankverbindungen:
Postbank Frankfurt * BLZ: 500 100 60 * Konto Nummer: 7535 89-600 IBAN DE75 5001 0060 0753 5896 00, BIC PBNKDEFF
Taunus Sparkasse Bad Homburg * BLZ: 512 500 00 * Kto: 1050478