iXactly
IT-Consulting GbR

Jacqueline Naumann

Die ganze Härte der ISO 27001

Ihr Untergang als Informationssicherheits-beauftragter (ISB)

Leitlinie Kompetenz Dokumentationsüberprüfung Verlinkung Bedrohung Terminsynchronisation Risikobeurteilungskriterien Schwachstellen Meldung Authentisierungsinformation Maßnahmenplanung Social Engineering Rechtevergabe Gesetze Zertifikat

Kurzüberblick

Liebe Leserin, lieber Leser,

vielen Dank, dass Sie sich für dieses Buch entschieden haben.

Informationssicherheit ist derzeit ein brennendes Thema, das vor allem durch das IT-Sicherheitsgesetz noch einmal an Fahrt aufgenommen hat.

Ich hoffe, ich kann Ihnen, liebe Informationssicherheitsbeauftragte und lieber Informationssicherheitsbeauftragter mit diesem Buch Unterstützung bieten, damit Sie Ihre Aufgaben auch unter erschwerten Bedingungen mit Eifer und Begeisterung weiterführen können.

Herzlichst, Ihre Jacqueline Naumann
Trainerin, Beraterin, Auditorin der iXactly IT-Consulting GbR

iXactly ist Ihr Dienstleister für Seminare, Beratung und Audits für Ihr ISMS.

Gostritzer Straße 61, 01217 Dresden

jacqueline.naumann@ixactly.com , www.ixactly.com

Vielen Dank
an Florentine Naumann für die Illustrationen im Buch!

Inhalt

Das scheinbar grenzenlose Universum an Aufgaben

Ihr Untergang als ISB

1 Einleitung

Möglicherweise spricht Sie dieses Buch an, weil Sie das Gefühl haben, in einem Universum an unzähligen Aufgaben-Galaxien zu versinken.

Das liegt daran, dass Sie nun mindestens das Grobgerüst Ihres ISMS aufgebaut haben und immer mehr Optimierungsaufgaben erledigen.

Dieses Buch ist für den Informationssicherheitsbeauftragten gedacht, der sein ISMS bereits seit über einem Jahr aufgebaut hat und nun eine gewisse Erschöpfung verspürt.

Das Buch soll Ihnen wieder Praxisbeispiele aus anderen Organisationen zeigen, damit Sie die bereits erreichte Qualität Ihres ISMS besser einschätzen können.

Liebe Informationssicherheitsbeauftragte, ich habe Ihr Buch dieses Mal streng nach GRC (Governance[1], Risikomanagement und Compliance) unterteilt. Im Governance-Teil erhalten Sie Praxisbeispiele aus der Planung und den Anforderungen eines ISMS. Im Risikomanagement-Teil finden Sie Praxisbeispiele aus den typischen Risikothemen und im Compliance[2]-Teil geht es um

die Einhaltung diverser Anforderungen aus Gesetzen, Verträgen oder einfach der ISO/IEC 27001.

1.1 Bekanntmachung mit unserem Buch-ISB

Im Buch werden viele Praxisbeispiele aus tatsächlich stattgefundenen Begebenheiten wiedergegeben. Um die Anonymität zu gewährleisten, nutze ich sogenannte schwarze Schafe, denen ich alle Kuriositäten unterschiebe.

Im Buch verwende ich die fiktive Organisation T34M. Die Organisation hatte bei ihrer Gründung Freude daran, die Buchstaben E durch 3 und A durch 4 zu ersetzen, so wie es einige angehende Hacker in der Sprache Leet tun.

Bei T34M arbeitet natürlich auch ein ISB, der hier T34M-L34D bezeichnet wird und der im Buch interviewt wird oder einfach Tatsachen erzählt.

T34M-L34D steht stellverstretend für hunderte Kunden, Kollegen, Mitarbeiter und Seminarteilnehmer, mit denen ich in den letzten 20 Jahren gesprochen oder denen ich einfach nur zugehört habe.

T34M-L34Ds Erzählungen sind Praxisbeispiele, die Ihnen zeigen sollen, dass sich in allen Organisationen teilweise recht kuriose Begebenheiten bezüglich Informationssicherheit ereignen.

T34M-BO$$ ist die oberste Leitung von T34M. Er kommt relativ wenig zu Wort, da T34M-L34D als ISB alle Aufgaben und Themen auf seinem Tisch hat und bearbeiten muss.

T34M-ADMIN ist als Administrator bei T34M beschäftigt.

T34M-EXTERNER ist ein fiktiver Dienstleister, dem alle Zitate von echten Dienstleistern untergeschoben werden.

1.2 Anonymität

Die vielen Zitate von Kunden, Lieferanten, externen Dienstleistern, ehemaligen Kollegen und auch Seminarteilnehmern sind anonymisiert. Für den Fall, dass Ihnen ein Zitat bekannt vorkommt, möchte ich anmerken, dass viele Herausforderungen nicht nur bei einer Organisation anzutreffen sind und sich deshalb Zitate auch ähneln können. Kein Leser muss in Sorge geraten, wenn er meint, sich in einem Zitat wiedererkannt zu haben. Die gesammelten Zitate umfassen einen zeitlichen Rahmen von über zwanzig Jahren.

1.3 Schwertsymbolik

Das Schwert des ISBs auf dem Cover versinkt sprichwörtlich in einer Aufgaben-Galaxie. Beginnen Sie gleich mit dem Lesen, um zu erfahren, unter welchen Bedingungen andere ISBs zu versinken drohten.

Viel Spaß beim Lesen und Lernen!

---

[1] Governance: Unternehmensführung, Erziehung

[2] Compliance: Einhaltung von Anforderungen aus Verträgen, Gesetzen und Normen

2 Scope-Ausschluss

Wann lohnt es sich, einen Scope[3]-Ausschluss zu definieren?

Die meisten Organisationen möchten mit einem Ausschluss Kosten sparen und bestimmen, welche Bereiche ein Zertifizierungsauditor nicht prüfen soll. Sehr oft werden Teile der Organisation dann ausgeschlossen, wenn sie nicht zwingend für die Wertschöpfung nötig sind.

Angenommen, bei Ihnen wäre die Urlaubsplanung in einer eigenen Abteilung angesiedelt, dann würde ich diese Abteilung aus dem ISO 27001-Geltungsbereich ausschließen. Einfach deshalb, weil Kunden nicht für eine sichere Urlaubsplanung bei Ihnen zahlen werden. Kunden interessieren sich für die Dienstleistungen, die diese bei Ihnen erwerben.

ISO/IEC 27001 Kap. 4.3 Festlegen des Anwendungsbereichs

Wären Sie allerdings eine KRITIS[4]-Organisation, bei der Schichtpläne zwingend erforderlich sind, dann müssten Sie selbst die Urlaubsplanung bei Ihrer Scope-Definition berücksichtigen.

Wie der Zertifizierungsscope lautet, bestimmen in aller Regel die Organisationen selbst. Manchmal werden

allerdings Begrifflichkeiten von den Zertifizierungsstellen abgelehnt.

Ihr Scope wird ganz sicher abgelehnt, wenn Sie beispielsweise folgenden Text auf Ihrem ISO/IEC 27001-Zertifikat stehen haben möchten: „Sichere Uhren nach ISO/IEC 27001“.

Die Ablehnung kommt zustande, weil die ISO/IEC 27001 Anforderungen an ein Managementsystem stellt und die Zertifizierung eines Managementsystems keine Produktzertifizierung ist. Weiterhin würde das Adjektiv „sichere“ abgelehnt, weil der Auditor nur das Managementsystem prüft und keine Produkteigenschaften. Er kann also nicht die Verantwortung für eine sichere Uhr übernehmen. Außerdem ist „sicher“ ein dehnbarer Begriff. Jeder könnte etwas anderes darunter verstehen. Und zu guter Letzt wird bei vielen Zertifizierungsstellen die Nennung der Norm, hier ISO/IEC 27001, abgelehnt.

Der Kunde soll beim Lesen des Scopes eine Vorstellung von Ihren zertifizierten Prozessen bekommen und nicht durch Normnennung getäuscht werden.