In 10 Schritten zur ISO-27001-Zertifizierung

Whitepaper

TEN Information Management GmbH

Altlaufstraße 40
85635 Höhenkirchen-Siegertsbrunn
Tel: +49 (0) 8102 7278934-0
www.ten-im.com

Inhalt

Vorwort

Vielen mittelständischen Unternehmen, die sich erstmals mit der Zertifizierung eines Informationssicherheits-Managementsystems (ISMS) nach ISO 27001 beschäftigen, stellen sich die folgenden Fragen:

- Wie kommen wir möglichst pragmatisch und ressourcenschonend zu unserer Zertifizierung?
- Welche Schritte müssen wir unternehmen, um uns optimal vorzubereiten?
- Welche externe Unterstützung brauchen wir möglicherweise dafür?

Auf diese und weitere Punkte wollen wir im Whitepaper eingehen.

01. Was soll zertifiziert werden?

Ausgangspunkt jeder Überlegung ist die Frage: Was soll eigentlich zertifiziert werden? Zertifiziert werden immer die Organisation und deren methodische Herangehensweise an Informationssicherheit. Die ISO 27001 orientiert sich dabei am PDCA-Zyklus (Plan – Do – Check – Act, auch Deming-Zyklus genannt). Nicht zertifiziert werden hingegen Produkte und Services. Deshalb sind werbende Aussagen wie „ISO 27001 zertifiziertes Rechenzentrum" oder „ISO 27001 zertifiziertes Software X" irreführend.

Muss die gesamte Organisation zertifiziert werden? Nicht notwendigerweise. Möglich ist, nur einzelne Teile einer Organisation einer Zertifizierung zu unterziehen. Dies können Standorte, Geschäftsbereiche oder auch einzelne Technologiebereiche sein. Zu unterscheiden ist dabei auch zwischen dem Anwendungsbereich des ISMS selbst und dem Geltungsbereich des Zertifikats.

Der **Anwendungsbereich** des ISMS definiert, welche Teile einer Organisation nach den Vorgaben des ISMS arbeiten. Dabei ist meist wünschenswert, möglichst viele Teile der Organisation auf die gleiche Art und Weise zu steuern. Einheitliche Prozesse und einheitliche Schnittstellen schaffen letztlich ein gemeinsames Verständnis darüber, wie die Organisation funktioniert.

Der **Geltungsbereich** des Zertifikats beschreibt, welche Teile der Organisation durch eine unabhängige Zertifizierungsstelle geprüft wurden. Nur für diese Teile darf die Organisation bei erfolgreicher Zertifizierung damit werben, dass sie ein ISMS nach der internationalen Norm ISO 27001 eingeführt hat und aufrechterhält.

Anwendungsbereich des ISMS und Geltungsbereich des ISO-27001-Zertifikats sind in der Praxis oft deckungsgleich. Das muss aber nicht so sein. Beispielsweise kann der Anwendungsbereich des ISMS sich über weite Teile der Organisation erstrecken, während der Geltungsbereich des ISO-27001-Zertifikats nur einen geringen Ausschnitt der gesamten Organisation umfassen kann. Organisationen können sich etwa aus Kostengründen dazu entschließen, nur Teile der Organisation zertifizieren zu lassen.

Im ersten Schritt ist also festzulegen, was eigentlich genau zertifiziert werden soll. Als Daumenregel empfehlen wir unseren Kunden, den Anwendungsbereich des ISMS innerhalb der Organisation möglichst breit zu wählen, den Geltungsbereich des ISO-27001-Zertifikats jedoch auf das absolut erforderliche Minimum zu beschränken. Dies hilft dabei, Kosten zu sparen, da der Aufwand für die Zertifizierung im Wesentlichen durch die Anzahl der vom Geltungsbereich umfassten Mitarbeitenden sowie die Anzahl der Standorte beeinflusst wird.

02. Dokumentation des Geltungsbereichs

In der Vorbereitung zur Zertifizierung muss die Frage geklärt werden, welche Teile der Organisation vom Geltungsbereich des Zertifikats abgedeckt sein sollen. Der Anwendungsbereich des ISMS selbst kann, wie oben beschrieben, durchaus größer und breiter gefasst sein.

Im nächsten Schritt ist also der Geltungsbereich des späteren Zertifikats zu dokumentieren. Dabei empfiehlt es sich, nicht nur zu beschreiben, welche Geschäftsbereiche, Standorte, Systeme, Technologien oder andere Aspekte der Geltungsbereich des späteren Zertifikats umfassen soll – sondern auch explizit zu dokumentieren, welche Teile der Organisation nicht enthalten sind. Diese Beschreibung hilft später, mit der Zertifizierungsstelle gemeinsam eine angemessene Herangehensweise für das Audit festzulegen.

Je besser abgegrenzt wurde, was alles zum Geltungsbereich gehört und was nicht, umso einfacher fällt es später, den Auditoren gegenüber zu argumentieren, welche Aspekte Gegenstand einer Prüfung sind – und welche eben nicht.

03. Abgleich der Norm-Anforderungen mit den eigenen Abläufen

Als Nächstes sollten die Anforderungen der Norm studiert und mit den Abläufen in der eigenen Organisation abgeglichen werden. An welchen Stellen gibt es Verfahren – beispielsweise aufgrund schon vorhandener Managementsysteme – die wiederverwertet werden können?
Welche Abläufe sind zu überarbeiten, da sie nicht konform mit den Normanforderungen sind?
Und an welchen Stellen ist die Organisation „komplett blank" und muss auf der „grünen Wiese" neue Verfahren implementieren?

Dies kann keine One-Man- beziehungsbeziehungsweise One-Woman-Show sein. Informationssicherheit aufzusetzen und kontinuierlich aufrechtzuerhalten, ist eine Teamaufgabe, die nicht bei einer einzelnen Person abgeladen werden kann. Empfehlenswert ist, eine Organisationsform zu definieren, die sich fortlaufend um das Thema Informationssicherheit innerhalb der Organisation kümmert.
Der oder die Informationssicherheitsbeauftragte ist dabei die Koordinationsstelle, die sich um die organisatorischen Aspekte kümmern sollte.

04. Dokumentation des Management-Systems

Managementsysteme erfordern Dokumentation, um zertifiziert werden zu können – das gilt auch für ISMS. Wie die Dokumentation geführt wird, lässt die Norm allerdings offen. Theoretisch ist eine Loseblattsammlung vorstellbar, sofern sie alle relevanten Aspekte enthält. In der Praxis wird man davon absehen wollen. Auch die in vielen Organisationen noch verbreiteten SharePoint-basierten Office-Dokumente haben Nachteile: Die Versionierung ist schwierig, Verlinkungen sind nur eingeschränkt möglich – und es kommt immer wieder zu Missverständnissen bei der Frage, welches der Dokumente aktuell und für wen maßgeblich ist. Stattdessen bieten sich Lösungen wie beispielsweise Instant 27001 für die Dokumentation an.

Welche Dokumentationen sind nun erforderlich? Zunächst sind alle Vorgaben, die im Rahmen des Managementsystems an die Organisation gestellt werden, festzuhalten. Dabei handelt es sich im Wesentlichen um Richtlinien, Verfahren und Arbeitsanweisungen. Darüber hinaus sind Aufzeichnungen (als Records bezeichnet) zu führen, mindestens zu etwaigen Informationssicherheits-Vorfällen sowie allen Änderungen, die eine Auswirkung auf die Informationssicherheit der Organisation haben können.

05. Umsetzung

Die Dokumentation ist aufgebaut und die Abläufe sind beschrieben. Jetzt gilt es, alles auch im betrieblichen Alltag umzusetzen. Dabei sind Nachweise dafür zu erstellen, dass eine bestimmte Aktivität tatsächlich durchgeführt wurde. Erst mit dieser operativen Durchführung entsteht für Organisationen der Mehrwert eines ISMS: Werden die Abläufe, die im ISMS dokumentiert sind, auch wirklich eingehalten, erhöht sich das Informationssicherheits-Niveau der Organisation. Ohne diesen Schritt wird das ISMS ein Papiertiger bleiben – das fällt erfahrenen Auditoren üblicherweise recht schnell auf.

Hier sind Organisationen im Vorteil, welche die Dokumentation mit einem Werkzeug wie Instant 27001 aufgebaut haben. Aufzeichnungen können dort direkt dokumentiert und Nachweise hochgeladen werden. Instant 27001 fungiert damit als zentraler Ablageort. Dies erleichtert nicht nur das jährliche Audit, sondern auch die unterjährige Arbeit: Die Mitarbeitenden wissen genau, wo sie für die Maßnahmen in ihren jeweiligen Verantwortungsbereichen die Dokumentation abzulegen haben.

Eine der wichtigsten Aufgaben bei der Umsetzung ist die operative Durchführung des Informationssicherheits-Risikomanagements. Die Norm fordert, Informationssicherheits-Risiken methodisch zu erheben, zu dokumentieren, zu bewerten und geeignete Maßnahmen zu ihrer Adressierung zu ergreifen. Hierfür kann der Anhang A der Norm herangezogen werden, der eine Sammlung von Maßnahmen enthält, die viele Risiken abdecken. Grundsätzlich können auch andere Maßnahmenkataloge verwendet werden.

06. Internal Audit durchführen

Mindestens einmal im Jahr muss die Organisation eine Überprüfung ihres ISMS hinsichtlich der Normkonformität durchführen. Wie lässt sich dies am besten bewerkstelligen? (Größere) Organisationen, die über geeignete qualifizierte und neutrale eigene Auditoren verfügen, können das Interne Audit selbst durchführen. Organisationen, die diese Personalressourcen nicht haben, können und sollten die Durchführung einem erfahrenen externen Auditor übertragen. Insofern bedeutet der Begriff „Internes Audit" nicht, dass dieses zwingend durch eigenes (internes) Personal durchgeführt werden muss; er dient vielmehr der Unterscheidung vom Audit durch die Zertifizierungsstelle.

Viele Organisationen betrachten das Interne Audit als lästiges Übel, das im Vorbeigehen von einem Mitarbeiter der Organisation mit erledigt werden kann. Dem ist nicht so. Die Zertifizierungsstelle wird beim späteren Zertifizierungsaudit fragen, ob der interne Auditor zum einen angemessen qualifiziert ist – und zum anderen über die entsprechende Unabhängigkeit verfügt. Insbesondere Letzteres ist regelmäßig nicht der Fall, wenn ein Angehöriger der Organisation, der womöglich bei der Umsetzung des ISMS mitgewirkt hat, das Interne Audit durchführt. Die oft und viel zitierte Funktionstrennung *(segregation of duty)* ist dann nicht gewährleistet. Am Internen Audit zu sparen, ist daher an der falschen Stelle gespart.

Beim Internen Audit wird gemäß einem durch die Organisation zu erstellenden Auditprogramm die Umsetzung der Normanforderungen im eigenen ISMS überprüft. Der interne Auditor nimmt dabei die neutrale Perspektive eines Dritten ein und prüft unvoreingenommen die Abläufe des ISMS. Er verfasst über das Ergebnis einen Bericht, der zum einen als Basis für Verbesserungen in den Wochen und Monaten nach dem Internen Audit dient. Zum anderen – wichtig! – muss dieser Bericht beim späteren offiziellen Zertifizierungsaudit als Nachweis, dass ein Internes Audit durchgeführt wurde, vorgelegt werden. Ein fehlender Nachweis führt regelmäßig zu einer Hauptabweichung im Zertifizierungsaudit.

07. Einen Management Review durchführen

Ein wichtiger Bestandteil des ISMS sind regelmäßige Berichte über den Stand der Informationssicherheit in der Organisation. Hierbei soll mindestens einmal im Jahr mit einem Verantwortlichen der obersten Leitung ein Austausch stattfinden, bei dem über relevante Themen der Informationssicherheit gesprochen wird. Dieser Austausch fördert zum einen die Verantwortung der Leitung; Intention der Norm ist, dass sich das Management aktiv mit den Themen beschäftigt.
Die Informationssicherheit soll ein Forum erhalten, um wichtige Aspekte transparent machen zu können. Zum anderen sollen hier aktiv Entscheidungen, die Auswirkungen auf das ISMS selbst und das Informationssicherheits-Niveau der Organisation haben können, getroffen und in der Folge auch umgesetzt werden.

Für den Management Review gelten einige inhaltliche und formale Anforderungen. Insbesondere ist das Ergebnis nachvollziehbar zu dokumentieren, und der Nachweis ist bei der Zertifizierung vorzulegen.

08. Zertifizierungsstelle auswählen

Das ISMS ist aufgebaut, die Abläufe eingeübt und operationalisiert. Nun ist es an der Zeit, die Organisation zur Zertifizierung anzumelden. In einem ersten Schritt ist eine geeignete Zertifizierungsstelle auszuwählen. Wir empfehlen, mehrere Angebote einzuholen.
Die angefragten Zertifizierungsstellen fragen üblicherweise die Eckdaten der geplanten Zertifizierung ab – d. h., wie viele Mitarbeiter im Geltungsbereich des Zertifikats arbeiten, wie viele Standorte einbezogen sind sowie weitere für die Abschätzung des Aufwands maßgebliche Details.

Vor der Entscheidung für eine Zertifizierungsstelle sollten Organisationen unbedingt nicht nur die kommerziellen Rahmenbedingungen überprüfen, sondern auch geeignete Auditorenprofile sichten. Fragen Sie bei der potenziellen Zertifizierungsstelle explizit nach zwei oder drei Auditorenprofilen. Beachten Sie bei der engeren Auswahl geeigneter Auditoren unbedingt deren Erfahrungen in Organisationen ähnlicher Größe. So gehen Auditoren, die ausschließlich in Großkonzernen Erfahrungen gesammelt haben, möglicherweise mit unrealistischen Erwartungshaltungen an ein Audit in einer kleineren, mittelständischen Organisation heran.

Vereinbaren Sie mit den Auditoren in der engeren Auswahl kurze Kennenlerngespräche. Für den Erfolg des Zertifizierungsvorhabens ist es ein wesentliches Kriterium, dass der Auditor zu Ihrer Organisation „passt“. Gegenseitige Sympathie und die berühmte Chemie zwischen den Beteiligten sind nicht die einzigen, aber sehr wesentliche Parameter, die neben der fachlichen Qualifikation ein entscheidendes Kriterium für eine erfolgreiche Zertifizierung bilden.

09. Zertifizierungsaudit

Haben Sie eine Zertifizierungsstelle beauftragt und einen Auditor ausgewählt, geht es an die Vorbereitung des Audits. Der Auditor bzw. das Auditorenteam wird einen Auditplan erstellen, der den Leitfaden für das Audit darstellt. Achten Sie darauf, den Auditplan rechtzeitig, d. h. mindestens einige Wochen vor der ersten Auditaktivität, zu erhalten. Das Audit selbst unterteilt sich in zwei Stufen: In Stufe 1 (auch als Level 1 bezeichnet) wird die reine Dokumentenlage betrachtet; in Stufe 2 geht es in die Details, wobei auch Nachweise gesichtet werden. Hierfür müssen Sie beispielsweise Aufzeichnungen (Records) über durchgeführte Aktivitäten vorweisen. Achten Sie bei der Planung unbedingt darauf, genügend Zeit zwischen Stufe 1 und Stufe 2 vorzusehen. Dies ermöglicht es, etwaige notwendige Änderungen, die sich aus den Ergebnissen der Stufe 1 ergeben, mit genügend Zeit in das ISMS einzuarbeiten – bevor die Überprüfung in Stufe 2 ansteht.

Es kann vorkommen, dass das Managementsystem bereits in Stufe 1 als nicht zertifizierungsreif eingeschätzt wird. Dies passiert häufig dann, wenn wesentliche durch die Norm geforderte Dokumente nicht vorhanden sind. In einem solchen Fall wird die Zertifizierungsstelle empfehlen, vor der Anmeldung zu Stufe 2 die fehlenden Themen nachzuarbeiten. Eventuell ist eine Wiederholung von Stufe 1 erforderlich. Wurde diese erfolgreich durchlaufen, folgt üblicherweise mit einigen Wochen Abstand Stufe 2. Ob das Zertifikat erteilt wird, hängt von der Anzahl und Art der Abweichungen ab, die während des Audits festgestellt werden. Grundsätzlich wird bei einer oder mehreren Hauptabweichungen kein Zertifikat erteilt. Die Organisation muss nachbessern. In einem solchen Fall werden die identifizierten Hauptabweichungen in einem Folgetermin nochmals geprüft. Nebenabweichungen verhindern die Zertifizierung dagegen nicht.

Abweichungen zu den Normanforderungen wird das Auditorenteam nach dem folgenden Schema erfassen:

- NC1: Nebenabweichungen *(Minor Non-Conformity)*
  Abweichungen, die für sich einen Mangel im Hinblick auf eine Normanforderung darstellen, die Effektivität des ISMS als Ganzes jedoch nicht beeinträchtigen. Solche Nebenabweichungen sind üblicherweise nicht zertifizierungsverhindernd und müssen nach Absprache bis zu einem definierten Termin oder bis zum nächsten (Erhaltungs-)Audit behoben werden.
- NC2: Hauptabweichungen *(Major Non-Conformity)*
  Abweichungen, die so gravierend sind, dass die Effektivität des ISMS als Ganzes nicht mehr gewährleistet ist. Solche Abweichungen sind zertifizierungsverhindernd, d. h., sie müssen zunächst behoben und im Rahmen einer Überprüfung erneut bewertet werden, bevor ein Zertifikat vergeben werden kann.
- OFI: Empfehlungen *(Opportunity for Improvement)*
  Möglichkeiten zur Verbesserung, auf die der Auditor im Rahmen seiner Prüfungshandlungen hinweist. Wichtig: Obgleich die Organisation nicht verpflichtet ist, diesen Empfehlungen zu folgen, so ist doch nachzuweisen – üblicherweise bis zum nächsten (Erhaltungs-)Audit –, dass sich die Organisation mit ihnen beschäftigt hat. Üblicherweise geschieht dies im Rahmen der nächsten Management-Bewertung, sodass die OFIs im Protokoll erwähnt und die Entscheidung hinsichtlich des Umgangs mit ihnen dokumentiert wird.

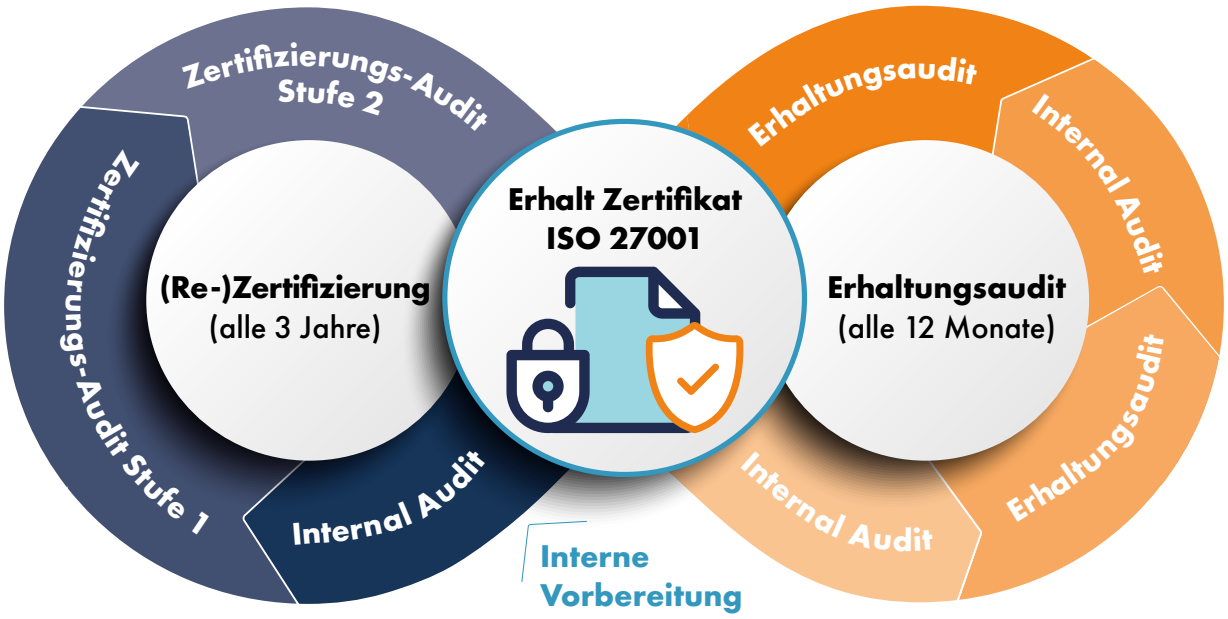
Auch mehrere Nebenabweichungen können in Summe bewirken, dass eine Hauptabweichung festgestellt wird – wenn sie beispielsweise so zahlreich sind, dass der Auditor die Effektivität des ISMS als Ganzes anzweifeln muss.

Unabhängig davon, ob die Organisation erstmalig oder wiederkehrend auditiert wird, sollten die Verantwortlichen nicht davon ausgehen, dass die Prüfungshandlung vollständig ohne Nebenabweichungen oder Empfehlungen vonstattengeht. Ein Auditbericht gänzlich frei von Feststellungen ist oft ein Zeichen dafür, dass nicht so genau hingesehen wurde.

10. Erhalt des Zertifikats

Nach erfolgreich absolviertem Zertifizierungsaudit erteilt die Zertifizierungsstelle ein Zertifikat, mit welchem die zertifizierte Organisation den Nachweis erbringen kann, ein ISMS eingeführt zu haben. Das Zertifikat kann auch auf der Webseite der Organisation verwendet werden, um Dritten gegenüber das ISMS nachzuweisen. Zertifikate enthalten üblicherweise eine Nummer, anhand derer Dritte die Gültigkeit des Zertifikats bei der Zertifizierungsstelle überprüfen können. Ebenso aufgeführt ist der vorher festgelegte Geltungsbereich des Zertifikats – zusammen mit der Geltungsdauer. Zertifizierte Organisationen sollten darauf achten, abgelaufene Zertifikate rechtzeitig durch neue zu ersetzen (s. auch folgender Abschnitt).

Zertifizierungzyklus ISO 27001



Zertifizierungsaudit erfolgreich – und jetzt?

Der Erfolg sollte gebührend gefeiert werden! Heben Sie die Teamleistung Ihrer Organisation hervor – und denken Sie schon jetzt an das Folgeaudit. Nach dem Audit ist vor dem Audit! Ein Zertifizierungszyklus dauert üblicherweise drei Jahre: Im ersten Jahr wird das vollständige Zertifizierungsaudit durchgeführt, in den beiden Folgejahren jeweils mit 12 Monaten Abstand ein sogenanntes Erhaltungsaudit. Hierbei werden ausgewählte Aspekte des ISMS geprüft. Auch hierfür sollten Sie frühzeitig mit der Zertifizierungsstelle Termine vereinbaren. Wichtig ist außerdem, darauf zu achten, dass der Auditor Ihnen den Auditplan rechtzeitig zukommen lässt. Nur dann kann sich Ihre Organisation angemessen vorbereiten. Ihr Auditor wird sich üblicherweise rechtzeitig vor dem Erhaltungsaudit mit Ihnen in Verbindung setzen und die geplanten Inhalte besprechen. Die Erhaltungsaudits sind in der Regel weit weniger umfangreich als das Zertifizierungsaudit und dienen auch dazu, etwaige Änderungen, die sich über die Zeit ergeben haben, dem Auditor und der Zertifizierungsstelle vorzustellen. Nach Ablauf der drei Jahre beginnt der Zyklus von vorne – und es steht ein erneutes vollständiges Zertifizierungsaudit an.

Wichtig für die kontinuierliche Verbesserung und die Erhöhung des Informationssicherheits-Niveaus ist, dass nach einem Audit die Organisation in der täglichen Umsetzung der Normanforderungen nicht nachlässt. Informationssicherheit ist ein kontinuierlicher Prozess – Organisationen, die immer erst kurz vor dem nächsten Audit versuchen, ihre Dokumentation zu „polieren", haben viel Aufwand mit der Zertifizierung – aber nur einen sehr überschaubaren Mehrwert.

Über TEN IM & unsere Leistungen

TEN Information Management ist ein modernes Dienstleistungsunternehmen für Informations- und IT-Sicherheit. Im Auftrag unserer Kunden führen wir Interne Audits von Informationssicherheits-Managementsystemen nach ISO 27001 durch. Unsere erfahrenen Auditoren geben dabei wertvolle Tipps, wie das ISMS verbessert werden kann. Sie verfügen über lange Berufserfahrung in der ISMS-Welt.

Bei der Dokumentation der Managementsysteme arbeiten wir schon seit mehreren Jahren mit dem spezialisierten Dokumentationssystem Instant 27001, das mittlerweile bei mehr als 1000 Unternehmen weltweit im Einsatz ist. Das Produkt ist in zwei Versionen verfügbar: zum einen für die beliebte Atlassian-Confluence-Plattform, zum anderen in einer Version für Microsoft 365, die eine vollständige Integration in die Arbeitsumgebung der jeweiligen Organisation bietet. Beiden Versionen gemeinsam ist die geführte Implementierung, bei der die Verantwortlichen in den Organisationen praktisch bei der Umsetzung der Normanforderungen begleitet werden. Wir sind überzeugt davon, dass sich die Konformität zu Managementsystem-Standards nicht auslagern lässt – Organisationen müssen sich selbst darum kümmern. Unsere Intention ist es nicht, unseren Kunden möglichst viel unserer Zeit zu verkaufen. Stattdessen möchten wir sie in die Lage versetzen, sich mit den Normanforderungen selbst zu beschäftigen und die Umsetzung anhand der praktischen Anleitungen in Instant 27001 in die Hand zu nehmen.

Selbstverständlich stehen wir mit Rat und Tat zur Seite, wenn unsere Kunden Unterstützung benötigen. Dafür stellen wir unsere Security Consultant on Demand (SCOD) Services zur Verfügung, die schnellen Support bei Fragen zur Informations- und IT-Sicherheit ohne langfristige Bindung und langwierige Vertragsverhandlungen bieten. Unsere erfahrenen Consultants helfen sowohl bei spezifischen Fragestellungen zu einzelnen Normanforderungen als auch bei der Implementierung von Maßnahmen aus dem Anhang A der Norm.

Wir freuen uns auf Ihre Kontaktaufnahme!

TEN Information Management GmbH

Altlaufstraße 40
85635 Höhenkirchen-Siegertsbrunn
Tel: +49 (0) 8102 7278934-0
www.ten-im.com