# ISO 27001

## Nutzen und Chancen eines Managementsystems gemäß ISO 27001 – Praxiseinsichten aus der Perspektive eines Auditors

www.tuv.com

TÜVRheinland®
Genau. Richtig.

# Inhaltsangabe

# I. Einleitung

## Komplexe IT-Systeme sind heute in der Lage eine Fülle an Informationen zu verarbeiten. Im Rahmen der digitalen Transformation und einer dynamischen Bedrohungslage wird es allerdings immer schwieriger, sensible Informationen, Prozesse und Systeme zu schützen.

Die ISO 27001 ist der weltweit anerkannte Standard für die aktive Steuerung von Informationssicherheit in Organisationen: Er beschreibt die Anforderungen an die Umsetzung sowie die Dokumentation eines Informationssicherheits-Managementsystems (ISMS). Mit einem ISMS gemäß der Norm ISO 27001 lassen sich Risiken minimieren und Sicherheitsverfahren in Bezug auf die Informationssicherheit etablieren, die zur nachhaltigen Optimierung der Qualität der Systeme in Organisationen beitragen.

„Tue Gutes und rede darüber“: Mit einer ISO 27001-Zertifizierung demonstrieren Organisationen nach innen wie nach außen, dass ihnen Informationssicherheit wichtig ist. Eine Zertifizierung wirkt vertrauensbildend auf Kunden wie Geschäftspartner.

# IT Risiken reduzieren mit einer ISO 27001-Zertifizierung


TÜVRheinland®
Genau. Richtig.

Mit der Sicherstellung der Verfügbarkeit von IT-Systemen und -Prozessen sowie der Vertraulichkeit der Informationen erfüllen Organisationen außerdem internationale Anforderungen. Dieses kann ein wertvoller Wettbewerbsvorteil beim Zugang zu neuen Märkten sein. Die Minimierung von Sicherheitsrisiken ist zugleich ein aktiver Beitrag zum Markenschutz und dem damit verbundenen Reputationsmanagement. Die mit einem ISMS einhergehende Optimierung der Strukturen ist erfahrungsgemäß auch mit einer Senkung der Kosten verbunden.

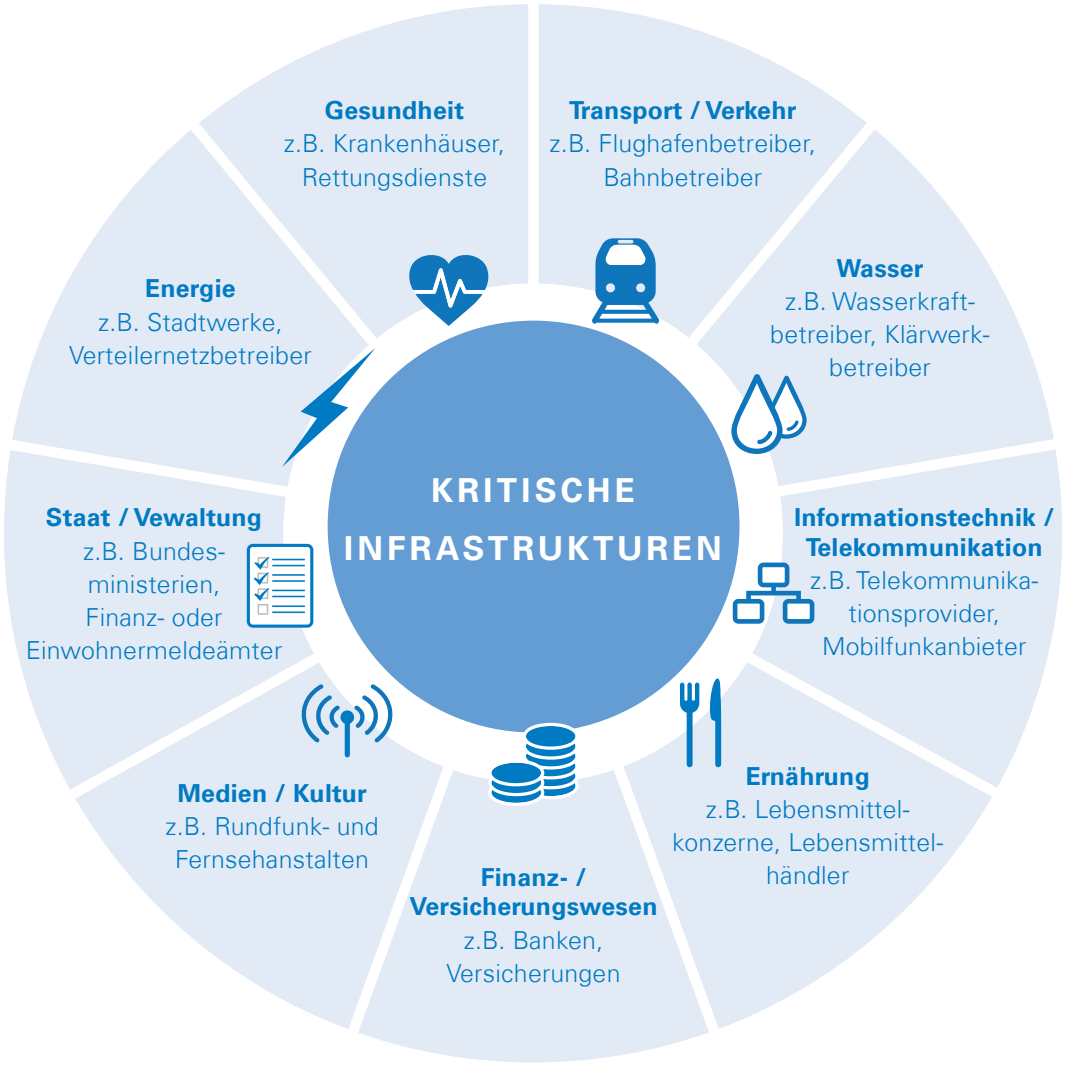
Kurz: Eine Norm, viele Vorteile.

## Audit- und Zertifizierungsablauf bei der ISO 27001


TÜVRheinland®
Genau. Richtig.

Betreiber **„Kritischer Infrastrukturen" (KRITIS)** und Unternehmen aus wichtigen Wirtschaftsbereichen wie Energieversorger oder Banken sind nach dem IT-Sicherheitsgesetz der Bundesregierung ohnehin verpflichtet, ein Mindestmaß an IT-Sicherheit zu gewährleisten und dies auch nachzuweisen. Viele Experten verstehen dies als Anforderung, ein ISMS einzuführen und dieses auch zertifizieren zu lassen.

> **WHITEPAPER FÜR DIE ENERGIEWIRTSCHAFT:** Dies sind die Inhalte und Fristen




Übersicht darüber, was „Kritische Infrastrukturen" (KRITIS) umfassen

# Vorteile einer IT-Sicherheitszertifizierung für Strom- und Gasnetzbetreiber


Erfüllung der Anforderungen des IT-Sicherheitskatalogs gem. § 11 Abs. 1a EnWG


Erhalt eines gesetzlich vorgeschriebenen Zertifikats


Sicherstellung Ihrer zu schützenden Systeme und Daten


Prozessverbesserung und Produktivitätssteigerung


Reduzierung der Haftungsrisiken


Wettbewerbsvorteil


Imagesteigerung in der Öffentlichkeit und bei Geschäftspartnern


Erfüllung der Kundenerwartungen

KRITIS-Betreiber in den Sektoren Energie, Wasser, Ernährung, Informationstechnik und Telekommunikation müssen bis zum 02.05.2018 und die Sektoren Finanz- und Versicherungswesen, Gesundheit sowie Transport und Verkehr bis zum 30.06.2019 die vorgesehenen Maßnahmen umsetzen.

# II. Zielsetzung dieses eBooks

## Mit diesem eBook wenden wir uns an alle, die ein berechtigtes Interesse an der Sicherheit von Informationen und IT-Infrastrukturen haben:

An Organisationen jeder Größe, an Privatwirtschaft wie Öffentliche Hand, aber durchaus auch an Endverbraucher, die einem laxem Umgang mit sensiblen personenbezogenen Daten zunehmend kritischer gegenüber stehen und bei denen Informationssicherheit auch stetig mehr die Kaufentscheidung beeinflusst.

Anhand konkreter Einblicke in die Norm ISO 27001 und die gelebte Praxis von Informationssicherheit in Organisationen, wie wir sie aus der unabhängigen Auditoren[1]-Perspektive seit Jahren und Jahrzehnten erleben, möchten wir zu einer aktiven Auseinandersetzung mit dem Thema Informationssicherheit anregen. Welche Anforderungen und internationale Standards in punkto Informationssicherheit gibt es und wie werden sie im Alltag gelebt? Wie gehen wir als Organisation mit dem Thema um, wo haben wir noch einen Tunnelblick und können wir uns noch verbessern?

Es ist in unser aller Interesse, dass wir dem Thema Informationssicherheit mehr Bedeutung beimessen als bisher. Die Bedrohungslage wird sich mit der steigenden Vernetzung des digitalen Wandels im Internet der Dinge und der zunehmenden Industrialisierung von Hacker-Angriffen weiter verschärfen.

**> QUICK CHECK:**
Der Online-Check des TÜV Rheinland liefert Ihnen ebenfalls hilfreiche Infos über Ihren Informationssicherheitsstatus.

[1] Im Rahmen eines Audits wird untersucht, ob ein Unternehmen die Anforderungen eines Standards erfüllt. Die Audits werden von einem speziell hierfür geschulten Auditor durchgeführt.

# III. Hinweise zum Lesen dieses eBooks

## Dieses eBook ist kein Leitfaden zur Umsetzung der Managementnorm und kann die umfassende Auseinandersetzung mit der ISO 27001 nicht ersetzen.

Vielmehr versteht es sich als kompakter, leicht verständlicher „Stichwortgeber", sich die Anforderungen der ISO 27001 auszugsweise in Erinnerung zu rufen. Im Anschluss daran finden sich typische Findings aus unserer Auditoren-Praxis, mit denen wir dazu anregen möchten, die Maßnahmen im eigenen Hause auf Konformität mit der ISO 27001 zu überprüfen.

Organisationen, die noch kein ISMS implementiert haben, inspiriert es hoffentlich dazu, die Steuerung von Informationssicherheit im eigenen Hause systematisch in Angriff zu nehmen. Die nachfolgenden Abschnitte und Anforderungen der ISO 27001, die wir hier darstellen, orientieren sich allein an unseren Erfahrungen im Rahmen von Audits (Prüfverfahren) und Zertifizierungen, die Auswahl ist rein willkürlich. Einen Anspruch auf Vollständigkeit verfolgen wir mit diesem eBook nicht.

# IV. Herausforderungen und typische Schwach-stellen

Die Anforderungen der ISO 27001 und unsere Erfahrungen aus der Auditoren-Praxis

## 1. Verstehen der Erfordernisse und Erwartungen interessierter Parteien (4.2)

Neu ist, dass die ISO 27001 den bisherigen Kundenbegriff auf den der interessierten Parteien erweitert. Die Organisation muss die Stakeholder bestimmen, die für ihr Informationssicherheitsmanagementsystem relevant sind und die Anforderungen dieser interessierten Parteien mit Bezug zur Informationssicherheit ermitteln. Die Anforderungen interessierter Parteien können gesetzliche und regulatorische Vorgaben sowie vertragliche Verpflichtungen beinhalten.

**INTERESSIERTE PARTEIEN KÖNNEN SEIN:**

- Kunden
- Eigentümer
- Mitarbeiter
- Lieferanten
- Kooperationspartner
- Anteilseigner
- Kostenträger
- Banken
- Aufsichtsbehörden
- Vereinigungen
- Fach- und Berufsverbände
- Wettbewerber
- die Gesellschaft im allgemeinen

kurz alle, die einen Einfluss auf die Informationssicherheit der Organisation haben können.

**UNSERE ERFAHRUNGEN AUS DER AUDITOREN-PRAXIS**

Sich mit den „Erfordernissen und Erwartungen interessierter Parteien“ auseinanderzusetzen, ist eine neue und sehr sinnvolle Anforderung, mit der sich Organisationen auf den ersten Blick erfahrungsgemäß schwertun. Lange hatten Unternehmen oft ausschließlich die Zufriedenheit ihrer Kunden im Fokus. Stakeholder wie Mitarbeiter, externe Anbieter, Aufsichtsbehörden oder Belange der Gesellschaft, wie sie jetzt die so genannte High Level Structure fordert, fanden bis dato keine Berücksichtigung. Einmal fokussiert, finden Unternehmen im Rahmen einer systematischen Herangehensweise erfahrungsgemäß schnell zu den in Bezug zur Norm relevanten Erfordernissen und Erwartungen, die angesichts der immer häufigeren Sicherheitsvorfälle stetig zunehmen.

Zu den Schwerpunkten zählt unter anderem die Einhaltung gesetzlicher Vorschriften und Compliance. Das können Anforderungen aus dem IT-Sicherheitskatalog, dem Bundesdatenschutzgesetz, dem „Datenschutzanpassungs- und Umsetzungsgesetz (DSAnpUG)“ oder der EU-Datenschutzgrundverordung sein. Auch ethische Gesichtspunkte sowie Wahrung datenschutzrechtlicher Belange von Mitarbeitern sowie die Wahrung von Sicherheit, Vertraulichkeit und Integrität von Geschäftskundendaten spielen eine Rolle.

**FRAGEN ZUM THEMA INFORMATIONSSICHERHEIT UND ZERTIFIZIERUNG?**

Kontaktieren Sie uns einfach. Wir erstellen Ihnen gerne ein unverbindliches Angebot.

NEHMEN SIE KONTAKT MIT UNS AUF

## 2. Maßnahmen zum Umgang mit Risiken und Chancen (6.1)

Die ISO 27001 stellt unter anderem die Anforderung, dass sich Unternehmen aktiv mit ihrem Organisationszweck auseinandersetzen. Sie sollten sich der internen und externen Faktoren bewusst sein, die die Ziele ihres Informationssicherheitsmanagementsystems – also den Schutz von Werten, Daten, Prozessen und Systemen – beeinträchtigen können.

Das bedeutet, sie müssen analysieren, was ihre Informationssicherheit auf interner wie externer Ebene bedrohen kann, also seitens Mitarbeiter, externer Angreifer bzw. unautorisierter Dritter. Unternehmen sind gefordert, eine entsprechende Risikostrategie zu entwickeln. Dazu müssen sie

- die Risiken identifizieren und bewerten, welches Schadensausmaß sie für die Organisation haben können (Kritikalität),
- bewerten, wie hoch die Wahrscheinlichkeit ist, dass dieses Risiko wirklich eintritt,
- entscheiden, wie sie diese Risiken behandeln wollen (reduzieren, übertragen, vermeiden oder akzeptieren)
- und im Einklang mit den Normanforderungen entsprechende Maßnahmen daraus ableiten.

Ziel ist es, Unternehmen noch stärker für drohende Risiken zu sensibilisieren und sie zu einer bewussten Auseinandersetzung mit diesen anzuhalten und die Risiken aktiv zu steuern.

**UNSERE ERFAHRUNGEN AUS DER AUDITOREN-PRAXIS**

Bei der Erstellung der geforderten Risikoanalyse und der Bewertung der Risiken sollten sich Unternehmen nicht nur mit Schwachstellen der IT-Infrastruktur auseinandersetzen. Ein wichtiger Punkt bei einem ISMS ist auch die physische Sicherheit. Beim Abgleich mit den Normanforderungen in Bezug auf alle erforderlichen Maßnahmen zum Schutz der Organisation ist die Verwundbarkeit der Organisation in punkto physischer Sicherheit immer wieder ein Thema: Unternehmen wird bewusst, dass die physische Zutrittskontrolle zur Organisation möglicherweise Lücken aufweist. Damit bieten sie nicht nur Innentätern, sondern auch externen Angreifern ungewollt und vor allem unbewusst eine offene Flanke.

Ein „klassisches“ Beispiel dafür ist, dass es zwar meist eine zentrale Besucheranmeldung gibt, die den Zutritt zum Gebäude offiziell steuert. Konterkariert wird dies durch einen ungesicherten Nebeneingang, über den sich nicht nur die Raucher unter den Mitarbeitern, sondern auch ungebetene Dritte Zutritt zum Gebäude verschaffen können. Mögliche Folgen sind Datendiebstahl oder die Manipulation von Prozessen und Systemen bis hin zur Kompromittierung privilegierter Accounts.

## 3. Informationssicherheitsziele und Planung zu deren Erreichung (6.2)

Die ISO 27001 fordert, dass sich die Organisation konkrete Informationssicherheitsziele setzt. Diese müssen ...

- ... im Einklang mit der Informationssicherheitspolitik stehen,
- messbar sein und der Risikoanalyse und -strategie entsprechen.
- Darüber hinaus müssen sie kommuniziert werden und immer wieder der tatsächlichen Bedrohungslage angepasst werden.
- Die Organisation muss darüber hinaus dokumentieren,

    - welche Maßnahmen sie ergreift, um ihre Informationssicherheitsziele zu erreichen,
    - welche Ressourcen sie dafür einsetzt,
    - wer dafür verantwortlich ist, diese Maßnahmen zu überwachen,
    - wann diese Schutzmaßnahmen voraussichtlich abgeschlossen sind

  und wie die Ergebnisse zu bewerten sind.

Zentrales Instrument zur Dokumentation dieser Punkte ist der so genannte Managementbericht der Geschäftsleitung. Er stellt die Mindestanforderung für die erste Stufe der Zertifizierung dar. Schon durch einen Blick in das Inhaltsverzeichnis eines Managementberichts kann der Auditor feststellen, ob das eingeführte Managementsystem – übrigens gleich welcher Normforderung – funktioniert oder nicht. Denn der Report ist das Herzstück des Managementsystems: Er sollte

- den Status ergriffener Maßnahmen und deren Managementbewertungen beleuchten,
- die Entwicklung interner wie externer Themen, die das ISMS betreffen, dokumentieren,
- Informationen zu Audit-Ergebnissen und erreichten Informationssicherheitszielen liefern,
- die Rückmeldung interessierter Parteien sowie die Ergebnisse von Risikobeurteilungen enthalten.

Ist dieser zentrale Report nicht vorhanden oder beinhaltet er nicht die geforderten Informationen, hat die Organisation die Zertifizierung verfehlt. Das Audit muss wiederholt werden.

### UNSERE ERFAHRUNGEN AUS DER AUDITOREN-PRAXIS

Im Rahmen der Definition von Organisationszielen begegnen wir immer wieder dem Umstand, dass Unternehmen monetäre Kennzahlen dokumentieren nicht aber die Antworten auf die zentralen Fragen rund um den Schutz der Organisation: Wie oft sind wir angegriffen worden, wie oft hat jemand versucht, unser System zu hacken? Welches Sicherheitsziel verfolgen wir (am liebsten Zero) und was unternehmen wir, damit wir dies auch erreichen?

Stattdessen werden Kennzahlen der BWA (Betriebswirtschaftliche Auswertung) wie Turnover und Ebit im Managementbericht verdichtet. Da der Managementbericht im Audit eine zentrale Rolle spielt, wirft das nicht nur Fragen rund um die Wahrung der Vertraulichkeit sensibler Geschäftsdaten auf. Bei näherem Hinsehen zeigt sich immer wieder, dass Kennzahlen durchaus eine enge Verknüpfung zu verborgenen Problemen in der IT haben können, ein Zusammenhang, der sich der Organisation in der Innenansicht offenbar nicht immer zwingend erschließt. In einem Beispiel etwa zeigte sich, dass sich hinter einer vergleichsweise hohen Reklamationsquote ein Problem mit der Verfügbarkeit der IT verbarg, welches das Unternehmen bis zu 8 Prozent des Umsatzes kostete.

Durch gezielte Ursachenanalysen und Korrekturmaßnahmen konnte die Organisation diese Ausfälle auf unter 1 Prozent senken. Durch die Fokussierung des Managementberichts auf die tatsächlichen Ziele des ISMS und die Integration der Kennzahlen zu Vorfällen, Bewertung von externen Anbietern, Ergebnissen aus Lieferantenaudits etc. und die Veröffentlichung des Reports innerhalb der Organisation erreichte das Unternehmen bei Mitarbeiterinnen und Mitarbeitern einen erheblich höheren Grad an Sensibilisierung für die Informationssicherheitsziele und eine deutlich tragfähigere Basis für die neuen Zielvorgaben der Informationssicherheit.

### HABEN SIE FRAGEN ZUR ZERTIFIZIERUNG GEMÄSS ISO 27001?

Unser FAQ-Dokument liefert hilfreiche Antworten.

Zum FAQ-Dokument

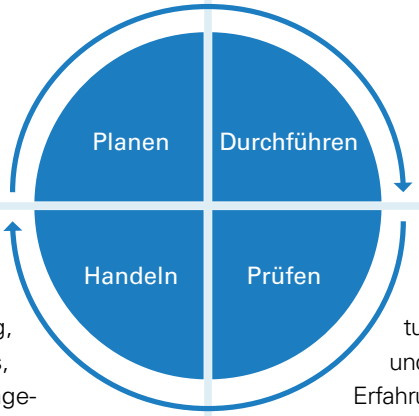
# 4. Verbesserung (10) - Nichtkonformitäten und Korrekturen (10.1)

Jedes Managementsystem zielt auf die kontinuierliche Verbesserung der Organisation ab.

**PDCA-ZYKLUS IN DER IT-SICHERHEIT**

Legen Sie die ISMS-Leitlinie sowie entsprechende Ziele, Prozesse und Verfahren fest, um Ergebnisse zu erreichen, die allen Grundsätzen und Zielen Ihres Unternehmens entsprechen.

Setzen Sie die im vorherigen Schritt definierten Punkte konsequent um.




Ergreifen Sie Maßnahmen zur Korrektur und Vorbeugung, basierend auf internen Audits, der Kontrolle durch das Management und weiteren eigenen Erkenntnissen » **kontinuierlicher Verbesserungsprozess (KVP).**

Schätzen Sie die Prozessleistung anhand der ISMS-Leitlinie und - Ziele sowie Ihrer eigenen Erfahrungen aus der Praxis ein (ggf. sind Messungen erforderlich). Leiten Sie die Ergebnisse an das Management zur Überprüfung weiter.

Tritt im Rahmen eines Auditverfahrens eine Abweichung von Maßnahmen und den damit verbundenen Zielen auf, handelt es sich um eine „Nichtkonformität". Die Organisation hat darauf mit Korrekturen und Maßnahmen der Überwachung zu reagieren. Sie muss außerdem die Ursache für die Nichtkonformität ermitteln, damit diese nicht erneut oder zu einem späteren Zeitpunkt an anderer Stelle auftreten kann.

Daneben hat die Organisation zu bestimmen, ob vergleichbare Nichtkonformitäten in der Organisation bestehen oder möglicherweise auftreten könnten. Bei der Einleitung von Korrekturen muss sie überprüfen, ob die Maßnahme wirksam ist. Korrekturmaßnahmen müssen angemessen sein, können aber, sofern notwendig, bis zu einer Anpassung des Informationssicherheitsmanagementsystems reichen. Die Organisation muss sowohl die Nichtkonformität als auch die Korrektur und ihre Ergebnisse dokumentieren. Nicht jede Nichtkonformität ist ein

K.O-Kriterium für eine Zertifizierung oder eine Re-Zertifizierung. Wird die Nichtkonformität allerdings nicht behandelt, spricht das gegen die Erteilung des Zertifikats. Im Anschluss daran gibt es zwei Möglichkeiten. Das Unternehmen erhält 90 Tage Zeit für die Nachbesserung. Der Auditor entscheidet, ob die Korrekturen durch einen Nachweis dokumentiert werden (Dokumentenprüfung) oder durch ein Nach-Audit in der Organisation vor Ort.

### UNSERE ERFAHRUNGEN AUS DER AUDITOREN-PRAXIS

Die Handhabung von Nichtkonformitäten wird häufig mit falschen Korrekturen belegt. Das kann folgende Gründe haben:

1.) Die Organisation schöpft die Möglichkeiten der Ursachenfindung nicht aus.

2.) Die Korrektur wird ohne Rücksprache mit dem Prozess-Verantwortlichen definiert und umgesetzt.

**EIN BEISPIEL ZU PUNKT 1:**
Die Sicherheitsrichtlinie des Unternehmens verbietet den Einsatz von USB-Sticks. Die Assistentin der Geschäftsleitung hält sich nicht daran. Die Mitarbeiterin zu ermahnen, wäre die falsche Korrektur. Warum? Weil so nicht auszuschließen ist, dass sich die Nichtkonformität durch diese Mitarbeiterin wiederholt, aber auch Nachahmer an anderen Stellen im Unternehmen nicht auszuschließen sind. Die richtige Korrektur wäre, zu prüfen, wie die Verwendung von USB-Sticks technisch zu verhindern ist, z.B. indem man die Ports an den Geräten entsprechend sperrt.

**EIN BEISPIEL ZU PUNKT 2:**
In Unternehmen häufen sich die Kundenbeschwerden rund um das Ticketsystem, weil keine zeitnahen Feedbacks erfolgen. Ein Kunde meldet sich daraufhin gleich beim Geschäftsführer. Dieser legt – ohne Rücksprache mit dem Prozess-Verantwortlichen – sogleich, aber vorschnell, die Korrektur für den Fehler fest: Er bestimmt, dass der eingetragene verantwortliche Vertriebsmitarbeiter das Ticket bearbeiten muss.

Alle Vertriebsmitarbeiter – auch der verantwortliche aus unserer Kundenbeschwerde –, sind allerdings tagsüber beim Kunden vor Ort. Unvermeidlich folgen weitere Beschwerden, weil das Problem nicht wirklich gelöst wurde. Ein externer Berater stellt bei der Ursachenermittlung fest: Aufgrund des aktuellen Workflows können die Vertriebsmitarbeiter Tickets nie innerhalb von 24 Stunden bearbeiten. Als Korrekturmaßnahme werden das Ticketsystem und der damit verbundene Workflow verändert: Ein Back-Office-Mitarbeiter pro PLZ-Gebiet ist der verantwortliche Erstkontakt. Er erhält die erste Meldung über das Kundenticket und nimmt den Datenbankeintrag vor. Er startet die Ursachenanalyse und definiert in Zusammenarbeit mit dem Informationssicherheitsbeauftragten Korrekturmaßnahmen zur Vermeidung von Wiederholungsfehlern. Sollte der Back-Office-Mitarbeiter nicht innerhalb von 24 Stunden die Beschwerde bearbeiten, erhält der Vertriebsleiter des PLZ-Gebietes die erste Eskalation. Vergehen weitere 24 Stunden ohne Bearbeitung des Tickets wird der Geschäftsführer informiert. In wöchentlichen Security Meetings berichtet der Informationssicherheitsbeauftragte über die Anzahl und Art der Vorfälle sowie die Dauer der Bearbeitung bis zum Abschluss sowie über die Anzahl der Eskalationen. Diese Daten fließen in die Managementbewertung ein.

# 5. ANHANG A

Die ISO 27001 enthält einen Katalog mit Maßnahmen und Zielen (Anhang A), mit der die Organisationen die Informationssicherheit auf allen Ebenen steigern. Die Umsetzung der Vorgaben ist im Rahmen der Norm verpflichtend.

### 5.A.) ANHANG A – AUFGABENTRENNUNG (A 6.1.2)

Darin ist unter anderem festgelegt, dass Aufgaben und Verantwortlichkeitsbereiche, die miteinander in Konflikt stehen könnten, zu trennen sind. So soll verhindert werden, dass unbefugte Dritte aus Vorsatz oder Fahrlässigkeit Werte der Organisation ändern oder für eigene Zwecke missbrauchen. Mangelnde Aufgabentrennung ist immer ein K.O.-Kriterium gegen die Erteilung eines Zertifikats.

#### UNSERE ERFAHRUNGEN AUS DER AUDITOREN-PRAXIS

Im Rahmen eines Audits stellte sich heraus, dass ein Fachbereich Informationen dokumentiert und eingesetzt hatte, ohne dass der Informationssicherheitsbeauftragte diese hätte bewerten oder freigeben können. In diesem Falle ging es um das Freigabe-Formular für die Ausgabe von Computern und Tablets, also um Werte (Assets) der Gesellschaft mit einer hohen Relevanz für die Informationssicherheit der Organisation.

Üblicherweise gibt es für die Ausgabe solcher Werte einen Freigabeprozess, der in diesem Falle jedoch „ressourcenschonend“ umgangen wurde: Eine Kollegin aus der Beschaffung erstellte das Freigabeformular, gab das Tablet an sich selbst aus, unterzeichnete das Formular persönlich und heftete es sorgfältig ab. An keiner Stelle der „Warenausgabe“ war eine zweite, kontrollierende Partei im Unternehmen mit von der Partie. Nach Aktenlage wusste kein Dritter über die Ausgabe des Geräts Bescheid. Der Vorgang fiel nur deshalb auf, weil die Auditoren stets im ersten Schritt die Vorgaben, dann die Umsetzung und zur Abrundung die Nachweise dazu prüfen. Erfahrungsgemäß reicht oft schon eine Stichprobe, um zu ermitteln, wie die Organisation mit dem Thema Aufgabentrennung umgeht.

### 5.B.) ANHANG A – PERSONALSICHERHEIT (A 7)

Das Unternehmen muss gemäß ISO 27001 sicherstellen, dass Beschäftigte und Auftragnehmer ihre Verantwortlichkeiten verstehen und sie für die vorgesehenen Rollen geeignet sind. Das bedeutet: Das Unternehmen muss alle Personen, die sich um eine Vakanz bewerben, einer „Sicherheitsüberprüfung“ unterziehen. Damit soll unter anderem sichergestellt sein, dass der Bewerber nicht vorbestraft ist, sich an allgemeine ethische Grundsätze hält und auch moralisch geeignet ist, die geplante Tätigkeit im Unternehmen auszuüben. Fälle wie die Anstellung eines Mitarbeiters, der wegen Unterschlagung vorbestraft ist und über Versicherungsfälle entscheiden darf oder als Buchhalter in einem Unternehmen angestellt wird, sollen vermieden wer-den. Auf diese Weise sollen potenzielle Schäden von der Organisation abgewendet werden. Kann das Unternehmen diese Sicherheitsprüfung nicht nachweisen, handelt es sich faktisch um eine Nichtkonformität. Bei der nächsten Zertifizierung hat das Unternehmen ein Problem.

#### UNSERE ERFAHRUNGEN AUS DER AUDITOREN-PRAXIS

Diese Nichtkonformität ist bei vielen Unternehmen festzustellen, zumindest, wenn es um freie Stellen unterhalb der Abteilungsleiter-Ebene geht. Hier müssen Auditoren ein erhebliches Fingerspitzengefühl beweisen und die Gesamtverantwortung der Stelle bewerten. Der Grund: Die Forderung nach einer „Sicherheitsüberprüfung“ ist selbst nach Ansicht von Juristen kompliziert und vor dem Hintergrund der deutschen Rechtsprechung bzw. der europäischen Datenschutzgesetzgebung kaum zu realisieren. Unklar ist unter anderem, wie Unternehmen, – wenn sie etwa ein polizeiliches Führungszeugnis verlangen – , ihr berechtigtes Interesse an einer „Sicherheitsüberprüfung“ und der Abfrage personenbezogener Daten wirksam nachweisen können. Dazu kommt der „War of Talents“: Im Ringen um Fachkräfte sehen viele Unternehmen inzwischen von der „Sicherheitsprüfung“ ab, damit der Bewerber sich nicht der Konkurrenz zuwendet. Für die Informationssicherheit kann das fatale Folgen haben. Jeder Bewerber könnte der Innentäter von morgen sein, der Prozesse und Systeme des Unternehmens vorsätzlich oder fahrlässig kompromittiert.

#### MEHR INFOS ZU „KRITISCHEN INFRASTRUKTUREN“ GEWÜNSCHT?

Dann lesen Sie unser FAQ-Dokument.

Zum FAQ-Dokument

### 5.C.) ANHANG A – VERANTWORTLICHKEITEN FÜR WERTE (ASSETS) (A 8.1) UND INVENTARISIERUNG DER WERTE (ASSETS) (A 8.1.1)

Die ISO 27001 fordert, dass informationsverarbeitende Werte wie Computer oder mobile Geräte inventarisiert werden und dieses Inventar laufend zu pflegen ist. Für alle Werte, die im Inventar geführt werden, sind Zuständigkeiten zu benennen.

#### UNSERE ERFAHRUNGEN AUS DER AUDITOREN-PRAXIS

Vor allem bei kleinen oder mittelständischen Organisationen ist festzustellen, dass jeder, der einen Bedarf hat, die Werte selbst beschafft und diese in Empfang nimmt. Die Organisation geht jeweils davon aus, dass er diese Werte über die Buchhaltung auch inventarisiert. Ein häufiger Trugschluss, wie die Realität zeigt.

Darüber hinaus ist der Informationssicherheitsbeauftragte oft nicht in den Prozess einbezogen. Ein Beispiel: Eine Neueinstellung steht an. Der Geschäftsführer fordert im Einkauf die Einrichtung eines neuen Arbeitsplatzes an, damit der neue Kollege gleich am ersten Tag zügig starten kann. Der Einkauf händigt die Ressourcen der IT aus, damit der Rechner professionell aufgesetzt wird. Der Informationssicherheitsbeauftragte als unabhängiger Dritter wird nicht über die Neueinstellung informiert und auch nicht über die Ausgabe der ICT-Geräte durch die IT. Das ist in doppelter Hinsicht problematisch: Der Informationssicherheitsbeauftragte ist für die Verwaltung der IT-Werte zuständig und auch für die Prüfung und Freigabe der IT-Identität des neuen Mitarbeiters (Definition von Rollen und Berechtigungen im Identity- und Access-Management).

### 5.D.) ANHANG A – RÜCKGABE VON WERTEN (ASSETS) (A 8.1.2)

Bei Austritt aus dem Unternehmen haben die Beschäftigten und sonstige Benutzer, die zu externen Parteien gehören, sämtliche in ihrem Besitz befindlichen Werte der Organisation zurückzugeben.

#### UNSERE ERFAHRUNGEN AUS DER AUDITOREN-PRAXIS

Scheiden Mitarbeiter aus dem Unternehmen aus, kann die Rückgabe von Werten oft nicht erfolgen. Der Grund: fehlende Inventarisierung oder es wurde bei der Einstellung nicht festgehalten, welche Werte überhaupt übergeben wurden. Kleinere Organisationen verfügen oft auch nicht über eine Personalabteilung, die dies lenken könnte. Hinzu kommt, dass der Informationssicherheitsbeauftragte meist nicht rechtzeitig über das Ausscheiden des Mitarbeiters informiert wird. Der Grund sind schlechte oder nicht definierte Prozesse. Dies ist ein Phänomen, das bei Unternehmen, die bereits ein Qualitätsmanagementsystem nach ISO 9001 eingeführt haben, kaum auftreten kann, da hier der Fokus klar auf dem Thema „Prozesse“ liegt. Bei Organisationen mit einem Informationssicherheitsmanagementsystem gemäß ISO 27001 liegt der Scope auf Informationssicherheit im Allgemeinen. Im Fokus stehen die IT-Infrastruktur und die dafür zuständige Mannschaft. Nicht umsonst fordern Experten für Informationssicherheit den Aufbau einer risikobasierten Unternehmensarchitektur, der auch Prozesse und Verantwortlichkeiten der gesamten Organisation in die Betrachtung miteinbezieht.

### 5.E.) ANHANG A – INFORMATIONSKLASSIFIZIERUNG (A 8.2)

Die Organisation ist für den Schutz der Informationen, die im Unternehmen ausgetauscht werden, verantwortlich. Das bedeutet: Sie muss dafür sorgen, dass sensible Informationen vor dem unbefugten Zugriff oder der Offenlegung durch Dritte geschützt sind. Ferner soll die Organisation ein Schutzniveau sicherstellen, das den gesetzlichen Anforderungen, dem Wert der Information und ihrer Kritikalität angemessen ist.

#### UNSERE ERFAHRUNGEN AUS DER AUDITOREN-PRAXIS

Bei Begehungen stellen wir immer wieder fest, dass Dokumente vertraulichen Inhalts in der Papiertonne entsorgt werden, ohne sie zu schreddern. Die Reinigungskräfte entsorgen diesen „Müll" in den Papiertonnen auf dem Betriebsgelände. Mitarbeiter können diese Dokumente in ihrer Gesamtheit entnehmen und somit z.B. auch auf Gehälter der Kolleginnen und Kollegen schließen. Ferner geraten sie unter Umständen in Besitz von Informationen, die durch das Bundesdatenschutzgesetz als besonders schutzwürdig eingestuft sind. Dieses ist ein grober Verstoß gegen die Bestimmungen der ISO 27001.

### 5.F.) ANHANG A - ZUGANGSSTEUERUNG (A 9)

Die Organisation muss den Zugang zu Information und informationsverarbeitenden Einrichtungen aktiv steuern. Informationen und Rechner dürfen nicht uneingeschränkt für jeden erreichbar sein. Das bedeutet, dass die Organisation eine aktive Zugangssteuerung pflegt und über eine Zugangssteuerungsrichtlinie verfügt, die dokumentiert, wer welche Zugangsberechtigungen erhält und die jederzeit überprüfbar ist.

#### UNSERE ERFAHRUNGEN AUS DER AUDITOREN-PRAXIS

Bei der Prüfung der Zugangssteuerung stellen wir immer wieder eine mangelnde Systematik fest: Die Vergaben von Rollen und Rechten für die firmeneigenen Server erfolgen häufig ohne ausreichende Planung von Freigaben und Checklisten. Darüber hinaus findet auch hier keine Trennung der Aufgaben statt. Der IT-Administrator erteilt sich eigene Berechtigungen und nutzt diesen privilegierten Zugang auch für herkömmliche Tätigkeiten statt auf ein Benutzerkonto mit Einschränkungen umzusteigen. Das Risiko: Bei herkömmlichem Nutzerverhalten und dem Besuch sicherheitskritischer oder bereits kompromittierter Seiten ist eine Infektion des Unternehmensnetzwerks nicht ausgeschlossen. Angreifer können sich über den privilegierten Account des Admins gleich den direkten Weg in die IT-Infrastruktur verschaffen, Werte stehlen und Prozesse manipulieren bzw. stören bis hin zum kompletten Betriebsausfall.

### 5.G) ANHANG A - PHYSISCHE UND UMGEBUNGSBEZOGENE SICHERHEIT (A 11)

Die Organisation muss dafür sorgen, dass sich niemand unbefugten Zutritt zum Betriebsgelände verschaffen kann, damit weder Information und noch informationsverarbeitende Einrichtungen der Organisation beeinträchtigt oder beschädigt werden können.

#### UNSERE ERFAHRUNGEN AUS DER AUDITOREN-PRAXIS

Bei Begehungen sind wir bereits auf alte Festplatten in unverschlossenen Gitterboxen im Außenbereich gestoßen. Die Kollegen erklärten im Rahmen der Sicherung vor unbefugten Zugriff, dass diese Gitterboxen per Videokamera überwacht werden. Dieses bietet faktisch keinen Schutz gegen den Zugriff unbefugter Dritter und wäre höchstens forensisch im Falle eines Diebstahls verwertbar gewesen. Allerdings stellte sich auch heraus, dass die Videoüberwachung zu diesem Zeitpunkt bereits seit mehreren Monaten defekt war und nicht einmal diese Möglichkeit bestanden hätte. Darüber hinaus hatte die Organisation auch gegen die gesetzlichen Regelungen zur Kennzeichnungspflicht verstoßen.

# V. Fazit

## Die Beispiele zeigen: Wem seine Daten, Prozesse und Systeme wichtig sind, der muss Informationssicherheit wirklich ernst nehmen und sich mit den Normanforderungen der ISO 27001 intensiv auseinandersetzen.

**SIE HABEN NOCH FRAGEN?**

Wir freuen uns auf Ihre Nachricht. Gerne erstellen wir Ihnen ein unverbindliches Angebot.

NEHMEN SIE KONTAKT MIT UNS AUF

Ansonsten eröffnet man Innentätern wie externen Angreifern allzu leicht offene Flanken, die erhebliche Folgen wie Datenmanipulation und -diebstahl bis hin zur Sabotage haben können.

Zugleich verdeutlichen die Beispiele auch, dass gerade Informationssicherheit eine wiederkehrende Aufgabe des Managements ist, die regelmäßig auf den Prüfstand gehört. Fragen wie: Was sind unsere Sicherheitsziele und entsprechen die ergriffenen Maßnahmen noch der Gefährdungslage? sind zentral für den kontinuierlichen Verbesserungsprozess im Rahmen der ISO 27001. Wer diese Praxis pflegt, ist nicht nur gegenüber Cyber-Attacken besser gerüstet, sondern auch besser auf das nächste Audit oder die Re-Zertifizierung vorbereitet. Jenseits der gesetzlichen Verpflichtung, ein wirksames und zertifiziertes integriertes Managementsystem nachzuweisen, bietet ein ganzheitliches und umfassendes Managementsystem die besten Möglichkeiten für den Unternehmenserfolg und die Entwicklung der Organisation.

# VI. Über den Herausgeber

## TÜV Rheinland ist ein weltweit führender unabhängiger Prüfdienstleister mit über 140 Jahren Tradition.

Unsere Experten prüfen technische Anlagen, Produkte und Dienstleistungen, begleiten Projekte und gestalten Prozesse für Unternehmen. Seit 2006 ist TÜV Rheinland Mitglied im Global Compact der Vereinten Nationen für mehr Nachhaltigkeit und gegen Korruption.

Mehr unter www.tuv.com/iso27001

Für die inhaltliche Unterstützung bei diesem eBook bedanken wir uns herzlich bei Klaus Schneider(Auditor ISO/IEC 27001 & ISO/IEC 27001 EnWG, Auditor DIN EN ISO 9001, Energieeffizienz- und Umwelt-Auditor).

TÜV Rheinland Cert GmbH
Am Grauen Stein
51105 Köln
Tel.: +49 800 888 2378 (kostenfrei)
Fax: +49 800 888 3296 (kostenfrei)
tuvcert@de.tuv.com

www.tuv.com

TÜVRheinland®
Genau. Richtig.