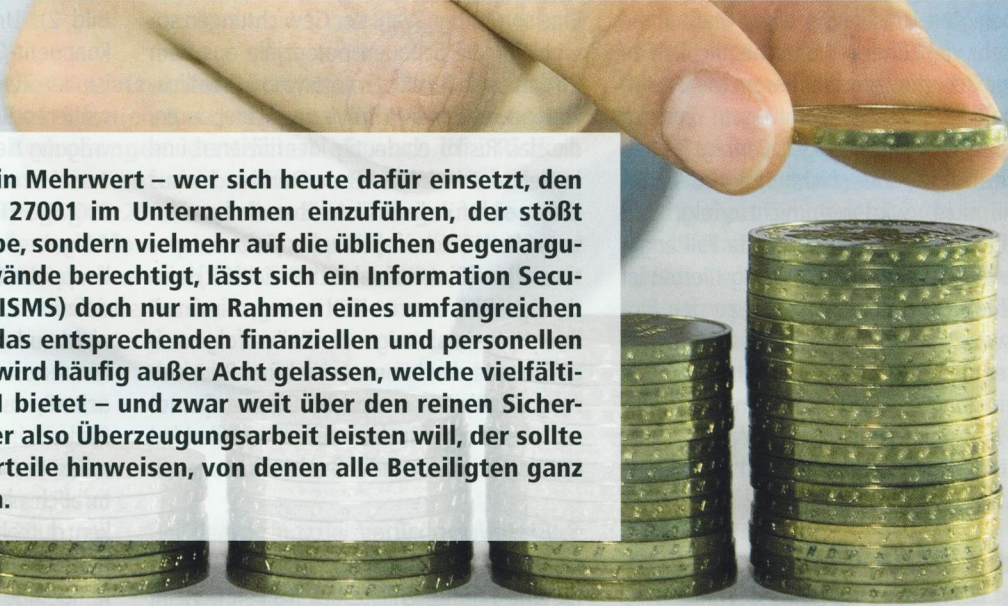


# Die Crux mit dem IT-Sicherheitsstandard ISO 27001

## Mehrwert ausschöpfen



**Zu teuer, zu aufwändig, kein Mehrwert – wer sich heute dafür einsetzt, den IT-Sicherheitsstandard ISO 27001 im Unternehmen einzuführen, der stößt häufig auf wenig Gegenliebe, sondern vielmehr auf die üblichen Gegenargumente. In der Tat sind Einwände berechtigt, lässt sich ein Information Security Management System (ISMS) doch nur im Rahmen eines umfangreichen Projekts implementieren, das entsprechenden finanziellen und personellen Aufwand erfordert. Dabei wird häufig außer Acht gelassen, welche vielfältigen Chancen die ISO 27001 bietet – und zwar weit über den reinen Sicherheitsaspekt hinaus. Wer hier also Überzeugungsarbeit leisten will, der sollte auf die vielen weiteren Vorteile hinweisen, von denen alle Beteiligten ganz konkret profitieren können.**

Bei der Erwägung, ob der IT-Sicherheitsstandard ISO 27001 in einem Unternehmen eingeführt werden soll, kommen fast immer nur die „belastenden“ Aspekte zur Sprache. Dabei gibt es in der Tat eine Reihe von Punkten, die auf der „Haben-Seite“ zu verbuchen wären. Für den Sicherheitsbeauftragten bietet sich beispielsweise die Chance, die eigene Position zu stärken und zu strukturieren. Denn sofern diese Rolle vor der Einführung von ISO 27001 überhaupt existiert, liegt ihr in den meisten Fällen kein Prozess zugrunde und daher auch kein konkret definierter Aufgabenbereich. Ein klar geregelter Sicherheitsprozess schafft hier Abhilfe: Er sorgt für ein effizientes Vorgehen und stellt sicher, dass alle relevanten Bereiche betrachtet werden.

Gleichzeitig hilft der Prozess, die Akzeptanz des Bereichs IT-Security innerhalb der Organisation zu erhöhen – denn häufig wird der Rolle des Sicherheitsbeauftragten von Seiten der restlichen IT-Belegschaft keine große Bedeutung beigemessen: In der Wahrnehmung vieler erschöpft sich der Bereich Sicherheit in der Installation von Anti-Viren-Software und der Konfiguration der Firewall. Darüber hinaus wird der Sicherheitsbeauftragte oft nur als Störfaktor wahrgenommen, der mit seinen Sicherheitsbedenken die Durchführung wichtiger Projekte bremst oder ganz verhindert.

ISO 27001 rückt den Bereich IT-Security ins rechte Licht: Hier wird Sicherheit nicht als einmaliges Projekt, sondern als kontinuierlicher Prozess betrachtet. Demensprechend ist der Sicherheitsbeauftragte als Prozessverantwortlicher zu sehen, der direkt der Geschäftsleitung unterstellt ist und in alle Projekte von Beginn an eingebunden wird. Auch der ganzheitliche Ansatz von ISO 27001 wertet seine Rolle auf: Das Aufgabenspektrum, das hier definiert wird, geht deutlich über rein technische Aspekte hinaus und umfasst auch Bereiche wie Personal oder Organisation. Demensprechend ist eine Zusammenarbeit mit den verschiedensten Unternehmensbereichen wie zum Beispiel der Rechtsabteilung, dem Controlling oder dem Risikomanagement erforderlich.

In seiner Funktion als Risikomanager blockiert der Sicherheitsbeauftragte Projekte nicht einfach nur, sondern ist vielmehr dafür zuständig, Risiken bewusst zu machen, Empfehlungen auszusprechen und so konstruktiv zur Projektplanung beizutragen.

### **Synergieeffekte und Prozessoptimierung: positive Nebeneffekte für die IT-Leitung**

Von einer verbesserten Wahrnehmung profitiert auch die IT-Abteilung als Ganzes, denn ISO 27001 macht die Abhängigkeit der Geschäftsprozesse von der IT direkt

sichtbar. So sieht die Norm unter anderem eine sogenannte Strukturanalyse vor, die aufzeigt, welche Systeme, Infrastrukturkomponenten, Anwendungen, Schnittstellen etc. konkret erforderlich sind, um bestimmte Geschäftsprozesse zu ermöglichen. Mit einer solchen Auflistung wird insbesondere der Geschäftsleitung der Stellenwert der IT als Wegbereiter für das Business deutlich gemacht.

Darüber hinaus hat die Strukturanalyse für die IT-Leitung noch einen weiteren, ganz praktischen „Nebeneffekt“: Sie liefert eine aktuelle Bestandsaufnahme der gesamten IT-Infrastruktur im Verbund inklusive aller Abhängigkeiten zwischen den Komponenten. Für viele Abläufe in der IT-Organisation sind dies äußerst wertvolle Informationen: Beispielsweise kann so bei der Störungsbehebung das Zusammenspiel einzelner Komponenten besser nachvollzogen werden. Im täglichen Betrieb fehlen häufig Zeit und Ressourcen, um die Infrastruktur-Daten immer auf dem aktuellen Stand zu halten – im Zuge der ISO-27001-Implementierung lassen sich solche Versäumnisse nachholen.

Ein weiterer Synergieeffekt, den sich die IT-Leitung zunutze machen kann, sind die Schulungsmaßnahmen, die ISO 27001 fordert. Damit sind nicht nur reine Sicherheits-

unterweisungen gemeint, sondern auch fachliche Schulungen, die auf den sachgerechten Umgang mit Systemen und Anwendungen abzielen. So sollen Ausfälle durch falsche Bedienung minimiert und letztlich die Verfügbarkeit erhöht werden. Das nützliche „Nebenprodukt“ für die IT-Leitung liegt auf der Hand: Geschulte Administratoren bringen Know-how in den IT-Betrieb, während der Support-Aufwand bei geschulten Anwendern deutlich sinkt.

Nützlich ist ISO 27001 auch für IT-Organisationen, die geordnete Betriebsprozesse im Rahmen des IT Service Management einführen möchten – denn hier schlägt der Standard bereits die richtige Richtung ein: ISO 27001 beschreibt bestimmte Prozesse, die zwar in erster Linie der IT-Sicherheit dienen, aber auch auf andere Bereiche der IT-Organisation ausgeweitet werden können

und so im ganzen Betrieb zur Optimierung von Abläufen führen. Das Störungsmanagement ist hierfür ein klassisches Beispiel: Für die Behebung von Security Incidents ist laut ISO 27001 ein entsprechender Prozess einzurichten. Allerdings sind Sicherheitsvorfälle nichts anderes als eine bestimmte Form von Störungen und können in weiten Teilen genauso abgearbeitet werden wie alle anderen Incidents im IT-Betrieb. Im Umkehrschluss lässt sich also im Zuge der ISO-27001-Implementierung ein umfassender Störungsmanagement-Prozess etablieren, der für die effiziente Bearbeitung aller Störungen sorgt.

Die Liste der Beispiele ließe sich beliebig fortführen: Ob Problem-, Änderungs-, Konfigurations- oder Verfügbarkeitsmanagement – letztlich profitiert die gesamte IT von der Einführung geordneter Prozesse.

Auch finanziell lohnt sich diese Standardisierung: Geregelt Schnittstellen zur IT und effizientere Abläufe reduzieren Overhead und Betriebskosten. Potential zur Kostenoptimierung ergibt sich zudem aus der bereits angesprochenen Strukturanalyse: Wer einen Überblick darüber hat, von welchen Systemen zentrale Geschäftsprozesse abhängen, der kann Investitionen in die IT-Sicherheit passgenau und effektiv planen.

### Compliance & Zertifizierung: Argumente für die Geschäftsführung

Mit dem Argument der Kostenoptimierung lässt sich häufig auch die Geschäftsführung überzeugen – genauso wie mit dem Stichwort Compliance: Die meisten Firmen

sind zur Implementierung bestimmter Sicherheitsvorkehrungen verpflichtet, sei es durch Gesetze wie etwa das Bundesdatenschutzgesetz oder aber durch branchenspezifische Regelungen wie „Basel II“ für das Finanzwesen oder das PCI-Regelwerk, das bei der Verarbeitung von Kreditkartendaten anzuwenden ist. All das sind Vorgaben, die sich mit einem ISMS nach ISO 27001 auf systematische Weise abdecken lassen. Und auch wenn bestimmte Maßnahmen nicht verpflichtend sind, so lohnt sich ihre Umsetzung in vielen Fällen trotzdem – denn die Außenwirkung einer sicheren IT-Infrastruktur ist nicht zu unterschätzen. In diesem Zusammenhang ist auch auf die Möglichkeit einer Zertifizierung hinzuweisen: Wer sich die Umsetzung von ISO 27001 und damit den sorgfältigen Umgang mit dem Thema IT-Sicherheit offiziell bestätigen lässt, der verfügt über ein schlagkräftiges Verkaufsargument und hebt sich so von Mitbewerbern ohne Zertifikat ab. Zudem lassen sich Sicherheitsaudits von Partnern und Kunden oft deutlich abkürzen, wenn die Organisation über ein gültiges Zertifikat verfügt.

Doch ob nun mit Zertifizierung oder ohne: An guten Gründen für die Einführung von ISO 27001 mangelt es in keinem Fall. Auf Gegenargumente wie „zu teuer“, „zu aufwändig“ und „kein Mehrwert“ bieten sie mit Sicherheit eine überzeugende Antwort. ■

### ISO 27001 im Überblick

Die internationale Norm ISO/IEC 27001 geht auf den British Standard BS7799 zurück und wurde 2005 als international anerkannter und zertifizierbarer ISO-Standard veröffentlicht. Sie ist zentraler Bestandteil der ISO-27000-Normenreihe, die Sicherheitsmaßnahmen für den Schutz der IT in den Bereichen „Vertraulichkeit“, „Verfügbarkeit“ und „Integrität“ definiert.

- Ganzheitlicher Ansatz: Mit dem Konzept eines Information Security Management System (ISMS) bietet ISO 27001 eine ganzheitliche Herangehensweise an das Thema Informationssicherheit. Betrachtet werden neben rein technischen Maßnahmen auch Bereiche wie Personal und Organisation.
- Kontinuierlicher Prozess: Die Norm basiert auf dem sogenannten PDCA-Kreislauf (Plan – Do – Check – Act): Dementsprechend definiert ISO 27001 die Entwicklung eines ISMS nicht als Projekt, sondern als dauerhaften Prozess, in dem das ISMS laufend überprüft und verbessert wird.
- Geschäftsprozess-Sicht: ISO 27001 setzt bei den Geschäftsprozessen an. Von deren Schutzbedarf ausgehend wird der Schutzbedarf zugrunde liegender IT-Infrastruktur ermittelt.



Für Abonnenten ist dieser Artikel auch digital auf [www.datakontext.com](http://www.datakontext.com) verfügbar



Weitere Artikel/News zum Schwerpunkt unter [www.datakontext.com/secman](http://www.datakontext.com/secman)



Marc Heinzmann,  
Geschäftsführer der  
plan42 GmbH

Brigitta Strigl,  
Beraterin bei der plan42  
GmbH