Die vierte industrielle Revolution beziehungsweise Industrie 4.0, welche die intelligente Vernetzung von Maschinen und Abläufen in der Industrie mit Hilfe von Informations- und Kommunikationstechnologie bezeichnet, hat längst begonnen.

Wir sind heute viel stärker abhängig von der Konnektivität der Unternehmen (dem Vernetzungsgrad), der ihr zugrundeliegenden Infrastruktur sowie der Nutzung des Internets und mobiler Geräte. Diese Abhängigkeit wurde aufgrund der Covid-19-Pandemie noch verstärkt und hat heute einen noch grösseren Bedarf an System- und Ausfallsicherheit digitaler Systeme zur Folge.

Carolina Klint, Risk Management Leader Continental Europe bei Marsh, sagt im Global Risk Report 2022, der angesichts des WEF veröffentlicht wurde: «Während sich die Unternehmen von der Pandemie erholen, richten sie ihren Fokus zu Recht auf die organisatorische Resilienz und die ESG-Leistung (Environmental Social Governance). Da die Cyberbedrohungen heutzutage schneller zunehmen als unsere Fähigkeit, sie dauerhaft zu beseitigen, ist ganz klar, dass es ohne glaubwürdige und durchdachte Pläne zum Cyberrisikomanagement weder Resilienz noch Governance geben kann.»

Cyberkriminelle agieren zusehends geschickter und treffen Unternehmen dort, wo sie am verletzlichsten sind. Der verursachte Schaden kann verheerende finanzielle Auswirkungen haben und den Geschäftsbetrieb sowie die Infrastruktur für Wochen lahmlegen.

Am 25. Mai 2018 wurde in Deutschland die DSGVO in Kraft gesetzt. Sie ist ein Compliance-Standard zur Verbesserung des Datenschutzes und gilt für alle Unternehmen innerhalb und ausserhalb der EU, die personenbezogene Daten von EU-Bürgern speichern oder verarbeiten.

Inzwischen wurde auch das Schweizer Datenschutzgesetz erneuert. Die Einführung des neuen Datenschutzgesetzes (DSG) ist für September 2023 vorgesehen.

Sowohl der ISO-27001-Standard also auch die DSGVO zielen darauf ab, die Datensicherheit zu verbessern, das Risiko von Datenschutzverletzungen zu minimieren und die Vertraulichkeit, Integrität und Verfügbarkeit sensibler Daten zu gewährleisten. Unternehmen sind aufgefordert, mögliche Risiken zu reduzieren. Das Augenmerk richtet sich auf versehentliche oder unrechtmässige Zerstörung, Verlust, Änderung, unbefugte Weitergabe von personenbezogenen Daten oder den Zugriff auf solche.

Internationale Normen bieten Lösungen, die es Organisationen ermöglichen, Rahmen und Systeme zur Bewertung und Bewältigung der Situation einzurichten – zum Schutz von Informationen, zur Sicherung von Anwendungen und Diensten sowie der Infrastruktur.

IT-relevante ISO-Standards

Hinter dem Begriff International Organization for Standardization (ISO) steht eine Organisation, die das Ziel der Schaffung von international einheitlichen Normen verfolgt.

Seit der Gründung der ISO-Organisation am 23. Februar 1947 in London wurden über 21'000 Normen veröffentlicht.

Die Standards, die für IT-Unternehmen interessant sein könnten:

- Sicherheit und Datenschutz für das Internet der Dinge (IoT),
- Sicherheit und Datenschutz für Big Data,
- Sicherheit und Datenschutz für künstliche Intelligenz und Schutz biometrischer Daten.

Ergänzt werden diese durch neuere technische Spezifikationen wie ISO/IEC TS 27570, die einen Leitfaden für den Schutz der Privatsphäre in Smart-City-Ökosystemen enthält, sowie ISO/IEC TS 27100, die beschreibt, wie robuste Cybersysteme zum Schutz vor Cyberangriffen geschaffen oder weiterentwickelt werden können.

Die dritte Ausgabe von ISO/IEC 27002 wurde im ersten Quartal 2022 veröffentlicht. Diese Norm befasst sich mit der Kontrolle der Informationssicherheit und wurde aktualisiert, um dem technologischen Fortschritt, den Geschäftsentwicklungen und -praktiken sowie neuen Gesetzen und Vorschriften Rechnung zu tragen. Darüber hinaus gibt es die ISO-Normen für

- ISO/IEC 27035 Incident Management,
- ISO 22301 Business Continuity Management,
- ISO/IEC 27031 Informationstechnik und IT-Sicherheitsverfahren.

Eine Reihe von Management-Normen helfen beispielsweise beim Aufbau von organisatorischer Resilienz oder dabei, Geschäftsunterbrechungen entgegenzuwirken und die Überlebensfähigkeit und die Governance (Unternehmensführung) zu gewährleisten. Dazu gehören:

- ISO 22301 Business Continuity Management Systems,
- ISO/IEC 27001 Information Security Management Systems,
- ISO/IEC 27014 Information Security Governance.

ISO-Zertifizierung

Eine wichtige Voraussetzung für die erfolgreiche Umsetzung eines ISO-Managementsystems ist die aktive Rolle des Managements. Nicht nur im Hinblick auf die Bereitstellung der finanziellen, zeitlichen und personellen Ressourcen, sondern auch in der Anerkennung der Notwendigkeit zur Einführung und Weiterentwicklung des Managementsystems.

Die Zertifizierung nach ISO 27001 beziehungsweise der Aufbau eines ISMS (Informations-Sicherheits-Managementsystems) ist die gängigste Zertifizierung im IT-Bereich hierzulande und ein weltweit angewandter Standard. Sie weist folgende Merkmale auf:

- Nachweis darüber, dass man über einen Plan verfügt, um alle notwendigen Vorkehrungen zu treffen, das Unternehmen vor Sicherheitslücken zu schützen.
- Bewusstsein schaffen für potenzielle Risiken, die ein Unternehmen bedrohen.
- Sensibilisierung aller Mitarbeitenden für die sicherheitsrelevanten Themen.
- Wettbewerbsvorteil.

Die Implementierung eines ISMS erfolgt idealerweise in Kombination mit ISO 9001 – Qualitätsmanagementsystem. Diese Norm beinhaltet alle strategischen und operativen Führungsprozesse von Personal- und Unterstützungsprozessen bis hin zur eigentlichen Leistungserbringung. ISO 9001 bildet die Basis und ist ideale Grundlage für den Aufbau eines integrierten Managementsystems.

ITIL VERSUS ISO 20000

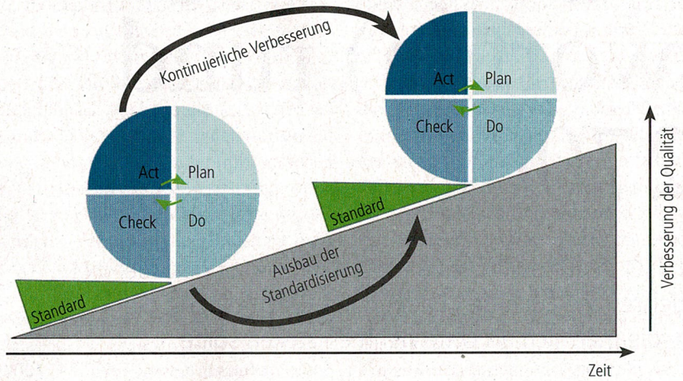
Während sich ISO 27000 vorwiegend auf die Datensicherheit konzentriert, sind andere Standards, wie ISO 20000 oder ITIL, auf das gesamte IT-Servicemanagement (ITSM) ausgelegt.

ITIL steht für Information Technology Infrastructure Library und ist eine Sammlung von Best-Practice-Prozessen, welche einen De-facto-Standard im Bereich IT-Services-Management bilden. Die Grundidee des ITIL-Frameworks besteht darin, Prozesse, Vorgehensweisen und Aufgaben aus dem Bereich ITSM in die Gesamtgeschäftsstrategie der Organisation zu integrieren, um so optimale Ergebnisse zu erzielen. Mit dem Aufkommen neuer Technologien wird ITIL regelmässig aktualisiert, so dass die existierenden Prozesse und Workflows noch besser verwaltet werden können.

Anders als ITIL adressiert die Norm ISO 20000 das Management von Firmen. Diese kann die Abläufe ihrer IT-Organisation nach den Anforderungen der Norm auditieren und zertifizieren lassen. Die ISO-Norm legt Mindestanforderungen für ein Service-Management-System fest und orientiert sich dabei zum Teil an den Management-Prozessen von ITIL.

ITIL kennt keine Zertifizierung von Unternehmungen, ist dafür jedoch in der Ausbildung von IT- und Management-Fachkräften stark vertreten. Mitarbeitende können sich ausbilden und ITIL-zertifizieren lassen, während mit der Auditierung einer ISO-Norm das Managementsystem der Unternehmung zertifiziert wird.

WEITERENTWICKLUNG DES MANAGEMENTSYSTEMS



Quelle: Attesta

Die kontinuierliche Weiterentwicklung des Managementsystems und damit einhergehend die Verbesserung der Qualität stehen im Zentrum einer ISO-Zertifizierung. Verbesserungspotenziale werden dabei anhand des PDCA-Kreislaufs (Plan-Do-Check-Act) identifiziert.

Der Zertifizierungsablauf

Ein ISO-Zertifizierungszyklus dauert drei Jahre. Die Gültigkeit der ISO-Zertifizierung wird anhand eines jährlichen, externen Audits überprüft und bei erfolgreichem Bestehen um ein weiteres Jahr verlängert. Im Zentrum dieses Prozesses steht die kontinuierliche Verbesserung (KVP) und Weiterentwicklung des Managementsystems.

Anhand der Durchführung von internen Audits – einem zentralen Instrument des Managementsystems – können die für ISO wichtigen Verfahren regelmässig und bereichsübergreifend überprüft werden. Neben der Einhaltung festgelegter Verfahren ist es wichtig, dass besonders die Mitarbeitenden sensibilisiert werden für die Bedeutung des jeweils eingeführten Standards im Unternehmen. Zentral ist dabei die Identifikation von Verbesserungspotenzialen anhand des PDCA-Kreislaufs (Plan-Do-Check-Act). Danach gilt es Lösungsideen zu entwickeln, sinnvolle Realisierungsschritte zu definieren, diese einzusetzen, sie zu überprüfen und dann die gewonnenen Erkenntnisse in die nächsten Planungsschritte einfliessen zu lassen. Dies ist ein Prozess, in den Mitarbeitende direkt einbezogen sind.

Die erforderlichen Dokumente für den Aufbau eines Managementsystems können selbständig oder mit Hilfe eines externen Beraters aufgebaut werden. Der zeitliche Aufwand variiert hier sehr stark und ist abhängig vom internen Know-how beziehungsweise demjenigen des externen Beraters. Analog dazu verhalten sich die Kosten.

Nach erfolgreicher Dokumentenprüfung kann das externe Audit mit einer Zertifizierungsgesellschaft geplant und festgelegt werden. Hierzu wird ein Auditprogramm erstellt, welches die zu beurteilenden Bereiche (Normkapitel), den zeitlichen Rahmen sowie die involvierten Personen ausweist.

Mehrwert einer ISO-Zertifizierung

Mit der Einführung eines ISO-Standards aus der ISO-27000-Familie leistet ein Unternehmen einen aktiven Beitrag zum Schutz der IT-Umgebung und zeigt gegenüber seinen Kunden und Partnern, dass es die Sicherheit seiner Daten und Informationen ernst nimmt und systematisch extern und unabhängig überprüfen lässt.

Aufgrund der zunehmenden Anzahl Hackerangriffe auf Schweizer Unternehmen und dem grösser werdenden Druck von Seiten DSGVO in Bezug auf den Umgang mit personenspezifischen Daten nimmt die Nachfrage nach ISO-27001-Zertifizierungen in der Schweiz deutlich zu. Eine erhöhte Nachfrage ist bei IT-Firmen, bei Start-ups beispielsweise in der Med-Tech-Branche, aber auch bei Lieferanten in kritischen Lieferketten und unterschiedlichen Branchen erkennbar – wie beispielsweise im Gesundheitswesen oder bei Logistikunternehmen. ■

DER AUTOR

Thomas Frischknecht,

Executive MBA HSG, ist Regionenleiter und Lead Auditor beim Unternehmen Attesta Schweizer Zertifizierungsgesellschaft. Seine Ausbildungsschwerpunkte liegen im Qualitätsmanagement – insbesondere ISO 27001 und Informationstechnologien. Er war langjähriger Geschäftsführer eines IT-Dienstleistungsunternehmens und selbständiger Unternehmer mit Beratungsschwerpunkten rund um IT-Sicherheit und CIO-Themen.