# ISO 27001: Betrieb, Bewertung, Verbesserung

**Nachdem wir in den vorangehenden Teilen alles vorbereitet haben, folgen nun der Betrieb, die Bewertung sowie die stetige Verbesserung des ISMS. Gemäss dem bekannten Demingkreis wurde das «Plan» umgesetzt, als nächste Schritte folgen Do, Check und Act.**

Das Normkapitel 8 verlangt die Planung der Schritte zur Zielerreichung des ISMS. Diese sind für jedes Unternehmen individuell, sollten aber immer in die gewohnten Betriebsabläufe integriert werden. Ob die Ziele erreicht wurden oder (noch) nicht, muss schriftlich festgehalten werden. Sollten noch nicht alle geplanten Schritte erfolgreich umgesetzt sein, gilt es die Abweichungen und die Gründe dafür zu bestimmen und anschliessend die weiteren Tätigkeiten zu steuern und so das ISMS stetig zu verbessern.

Fast alle kennen das, es kommt oft anders, als geplant. Jedes Unternehmen ist stetigen Veränderungen ausgesetzt. Dies hat immer auch Einfluss auf das ISMS. So gilt es diese ebenfalls zu erfassen und entsprechende Anpassungen vorzunehmen. Das ISMS ist keine jährliche oder gar einmalige Aufgabe, sondern stetigen Veränderungen unterworfen.

Weiter erfolgt nun die Durchführung der Risiko-Analyse gemäss den definierten Kriterien (siehe Maschinenbau 7/2018). Zuerst wird das Inventar erfasst, die Bedrohungen und Schwachstellen evaluiert und in einem nächsten Schritt die Eintrittswahrscheinlichkeit und die Auswirkung bewertet. Die Ergebnisse sind schriftlich festzuhalten.

Alle gemäss Kriterien nicht akzeptierten Risiken müssen behandelt werden, sei dies durch Vermeidung, Abwälzung auf Andere (Stichwort Versicherungen) oder einer Massnahme: die Anhänge A.5 bis A.18 zeigen 114 mögliche Kontrollen, wie auch die Grundschutzkataloge (neu Kompendium) des Bundesamts für Sicherheit in der Informationstechnik BSI umfassen mehrere hundert Massnahmen. Über die geplanten und umgesetzten Schritte muss Buch geführt werden.

## Bewertung

Ein wichtiger Punkt ist die regelmässige Bewertung des ISMS. Das Unternehmen definiert dabei, was, in welchem Rhythmus und durch wen überwacht und gemessen wird. Auch welche Methode dabei verwendet wird, wird selber definiert, zum Beispiel Interviews, Fragebögen, technische Messwerte usw.

Wichtig ist, dass vergleichbare und reproduzierbare Resultate erzielt werden. Die zu messenden Punkte sind dabei im Vorfeld zu definieren. Nachfolgend sind einige sogenannte KPIs (Key Performance Indicator) aufgelistet. Jedes Unternehmen muss aber für sich entscheiden, ob diese passend sind:

- Anzahl Verstösse gegen die Benutzer-Richtlinien
- Nicht eingehaltene Recovery-Zeiten gemäss BCM
- Anzahl falsch erfasster Tickets
- Anzahl Lieferanten/Partner ohne entsprechenden Vertrag
- Anzahl Sicherheitsverletzungen Intern
- Anzahl Sicherheitsverletzungen durch Externe
- Anzahl Abweichungen zur ISO-Norm
- Anzahl Personen ohne interne Awareness-Schulung
- Anzahl nicht rechtzeitig überprüfte Dokumente
- Anzahl falsch entsorgter Geräte, Festplatten, Mobile Geräte
- Anzahl falsch vergebener Berichtigungen (Systeme, File-Struktur usw.)
- Anzahl nicht begleiteter externe Personen

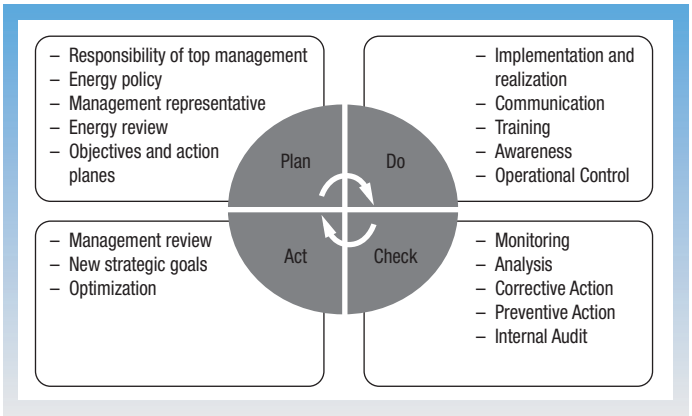
Bei allen Punkten gilt es zu definieren, welche Messwerte noch akzeptiert werden. Analog eines Ampelsystems kann zum Beispiel definiert werden: 1 = Grün, 2 bis 3 = Orange, >3 = Rot. Alle Resultate sind als Nachweis aufzubewahren.

Der zweite Punkt ist die regelmässige Kontrolle des ISMS. Mindestens jährlich ist das ISMS sowie die 114 Controls zu auditieren und damit zu zeigen, dass die Anforderungen aus der Norm auch entsprechend erfüllt werden. Dazu ist ein (oder mehrere) Auditplan zu erstellen. Darin sind die zu prüfenden Punkte, die Häufigkeit, die Methoden, die Verantwortlichkeiten sowie die Art des Berichtes zu definieren. Auch wenn der Normpunkt 9.2 «Internes Audit» heisst, kann er durch externe Spezialisten durchgeführt werden. Unter keinen Umständen darf die gleiche Person das Audit durchführen, die auch das ISMS unterhält, da diese Person nicht unabhängig und neutral ist. Dies ist aber ein wichtiger Erfolgsfaktor für das Audit. Ich empfehle sehr, dies entweder durch eine interne, unabhängige Person mit dem entsprechenden (Fach-)Wissen oder einer externen, auf ISO 27001/2 spezialisierten Firma durchzuführen. Natürlich macht es keinen Sinn, jedes Jahr alle Controls zu überprüfen. Wichtig ist aber, dass in einem Zertifizierungszyklus von drei Jahren alle Controls mindestens einmal überprüft werden. Idealerweise wird dies risikobasiert durchgeführt, das heisst, risikoreiche Bereiche werden regelmässiger überprüft als andere. Die Ergebnise sind schriftlich festzuhalten und dem Management zu präsentieren.

Hinweis: ein möglichlicher Auditplan kann beim Autor dieses Artikels kostenlos bestellt werden.

Der dritte Punkt des Kapitels «Bewertung» definiert Anforderungen an die Managementbewertung. Die Norm gibt klare Anforderungen, was darin enthalten sein muss. Ich empfehle sehr, alle verlangten Punkte in der Management-Präsentation aufzuführen, auch wenn nichts dazu gesagt werden kann. Folgende Punkte gilt es zu behandeln:

- Den Status aller Massnahmen, die definiert wurden, zum Beispiel aus Abweichungen bei Audits
- Alle Veränderungen von internen und externen Themen
- Rückmeldungen bei (Norm-) Abweichungen, aus den definierten KPIs, aus Audits und aus den definierten Zielen
- Rückmeldungen von interessierten Parteien (siehe Maschinenbau 5/2018)




Die vier Phasen des PDCA-Zirkels.

– Ergebnisse aus der durchgeführten Risiko-Analyse
– Möglichkeiten zur stetigen Verbesserung des ISMS

Alle besprochenen Punkte sowie die Entscheidungen daraus sind schriftlich als Nachweis festzuhalten.

## Verbesserung

Nur wer sich stetig verbessert, kann wachsen. Das gilt auch für das ISMS. Bei den Audits wird zwischen folgenden Abweichungen unterschieden:

– Hauptabweichung (Nichtkonformität): ein verlangter Normpunkt wird nicht erfüllt (zum Beispiel, wenn ein verlangtes Dokument nicht vorhanden ist)
– Nebenabweichung: ein verlangter Normpunkt wird zwar umgesetzt, entspricht aber nicht zu 100 Prozent den Erwartungen
– Verbesserung: der Auditor ist mit der Massnahme einverstanden, hat aber Vorschläge zur Erhöhung beziehungsweise Verbesserung der Informationssicherheit

Sollte dies der Fall sein, gilt es zuerst abzuklären, wie es zu dieser Abweichung kam. Allenfalls gibt es weitere Abweichungen, die im Audit nicht erkannt wurden, aber trotzdem vorhanden sind. Umgehend sind Korrekturen einzuleiten und die Wirksamkeit der getroffenen Massnahmen regelmässig zu bewerten. Das kann sogar dazu führen, dass Anpassungen am gesamten ISMS notwendig sind.

Wie bei allen Massnahmen muss die Wirtschaftlichkeit berücksichtigt werden. Es macht keinen Sinn, wenn ein möglicher Schaden CHF 1000 beträgt, die Tätigkeiten aber ein Mehrfaches davon kosten. Auch hier sind alle Abweichungen sowie die getroffenen Massnahmen schriftlich festzuhalten. Idealerweise wird ein Ticketing-Tool dafür zweckentfremdet. In einem Ticket kann sehr gut gezeigt werden, welche Schritte getroffen wurden, wer verantwortlich ist und wie der aktuelle Status der Massnahme ist.

Der letzte Normpunkt (10.2) umfasst einen einzigen Satz, der es aber in sich hat: «Die Organisation muss die Eignung, Angemessenheit und Wirksamkeit ihres ISMS fortlaufend verbessern.» Wie bereits mehrfach erwähnt, ist ein ISMS keine einmalige Sache. Stetig gilt es auf Veränderungen zu (re-)agieren und frühzeitig Korrekturen anzubringen. Nur ein gelebtes ISMS kann die Informationssicherheit für ein Unternehmen nachhaltig erhöhen.

Dies ist der letzte Artikel zur ISO 27001-Norm. In den kommenden Ausgaben widmen wir uns den 114 Controls. Folgende Fragen sollen geklärt werden: Was wird gefordert? Wie kann dies umgesetzt werden? Welche Werkzeuge stehen zur Verfügung?

**INFOS | KONTAKT**

**goSecurity GmbH**
Schulstrasse 11
CH-8542 Wiesendangen

Telefon +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch