ew Magazin für die Energiewirtschaft

Informationssicherheitsmanagementsysteme entsprechend ISO/IEC 27001

Nach der Zertifizierung ist vor der (Re-)Zertifizierung

Die Zertifizierung eines Informationssicherheitsmanagementsystems bis zum Januar 2018 dürfte bei den Energienetzbetreibern keine größeren Fragen mehr aufwerfen. Aber was muss nach diesem Stichtag beachtet und angepackt werden, um einen möglichst großen Nutzen aus dem implementierten System zu ziehen?

Während der Fokus der meisten Energienetzbetreiber im Augenblick noch auf dem erfolgreichen Abschluss der Zertifizierung liegt – oder nach erfolgreich abgeschlossener Zertifizierung zunächst einmal durchgeatmet wird –, lohnt es sich, einen Blick auf die Zeit danach zu werfen.

In der kommenden Phase ist mit der Planung entsprechender Maßnahmen ein Grundstein für die Weiterentwicklung des implementierten Informationssicherheitsmanagementsystems (ISMS) zu legen. Der Grundgedanke ist dabei, dass Informationssicherheit ein kontinuierlicher Prozess und kein einzelnes Projekt ist. Das heißt, dass das Thema nicht mit der Zertifizierung abgeschlossen ist. Mit einem ISMS muss zur Tagesordnung übergegangen und die Prozesse und Leitlinien dauerhaft im Unternehmen verankert werden. Das ISMS soll leben und sich an Veränderungen anpassen. Damit die Informationssicherheit nicht in einem unüberschaubaren Aufwand endet, sollten die im Folgenden beschriebenen Aktionsfelder für die Zeit nach der Zertifizierung zyklisch auf der Agenda stehen.

Reifegrad eines ISMS

Die erste erfolgreiche Zertifizierung bedeutet nicht, dass ein perfektes ISMS eingeführt ist, das keiner weiteren Aufmerksamkeit bedarf. Jetzt gilt es, eine möglicherweise als reine Pflichtübung betrachtete Einführung in einen Mehrwert für das Unternehmen zu verwandeln.

Die Weiterentwicklung des Managementsystems ist in der zugrundeliegenden ISO/IEC 27001 verankert – und zwar im PDCA-Zyklus (Plan-Do-Check-Act). Nach der Planung und Einführung eines ISMS ist eine permanente Überprüfung und Weiterentwicklung vorgesehen. Dieser kontinuierliche Verbesserungsprozess muss implementiert und gelebt werden.

Erfahrungsgemäß sind die Prozesse eines ISMS nach der Erstzertifizierung nicht ausgereift und erfordern einen verhältnismäßig hohen Aufwand bei der Durchführung. Beim Verbesserungsprozess sollte in den ersten Optimierungsschritten der Fokus auf die Prozesseffizienz gelegt werden, um Handlungsraum zu schaffen für die nächsten Entwicklungsstufen des ISMS.

Ähnlich vieler anderer Unternehmensbereiche kann die Qualität eines Managementsystems in verschiedene Stufen eines Reifegradmodells eingeordnet werden. Es existieren vielfältige Ansätze der Einstufung – hier sei beispielhaft auf die in Cobit v5 als Rahmenwerk der Governance in der Unternehmens-IT verwendeten fünf Stufen verwiesen (*Bild 1*). Dort reichen die Auswirkungen von reinen Auditfunktionen, also der Bestätigung, dass zu einem gegebenen Zeitpunkt bestimmte Vorgaben eingehalten werden, bis zu einer effizienten Steuerung der gesamten Unternehmens-IT in der höchsten Ausbaustufe.

Weiterentwicklung, Ausweitung und Integration

Parallel zur Etablierung eines kontinuierlichen Verbesserungsprozesses, der die Effizienzsteigerung der etablierten Prozesse des ISMS zum Ziel hat, ist eine zyklische Überprüfung der Risikoanalyse vorzusehen. Nur eine regelmäßige

de Normen aus der Reihe, die Unterstützung bei einzelnen Komponenten des ISMS bieten. So sind zum Beispiel in der ISO/IEC 27005 Beschreibungen des Risikomanagementprozesses und der Schritte der Risikoanalyse enthalten, in der ISO/IEC 27033 Beschreibungen zur Netzwerksicherheit.

Die Vorteile einer Ausweitung des ISMS auf ausgewählte, nicht normative Anteile liegen in der Nutzung der Erfahrung und der Spezialisierung, die in die Entwicklung dieser Normen eingeflossen sind, sowie in der Vergleichbarkeit des implementierten Managementsystems. Dadurch ist die vom Management durchzuführende Bewertung des ISMS deutlich vereinfacht.

Der zweite Hauptbereich der Weiterentwicklung eines ISMS ist die Integration in bestehende Managementsysteme. Es kann beispielsweise geprüft werden, ob und wie andere bestehende Managementsysteme – zum Beispiel ein Qualitätsmanagementsystem nach ISO/IEC 9001 oder ein Umweltmanagementsystem nach ISO/IEC 14001 – mit einem ISMS in ein integriertes Managementsystem (IMS) überführt werden können. Dabei werden die Methoden, Prozesse und Instrumente der einzelnen Systeme in einer einheitlichen Struktur zusammengefasst.

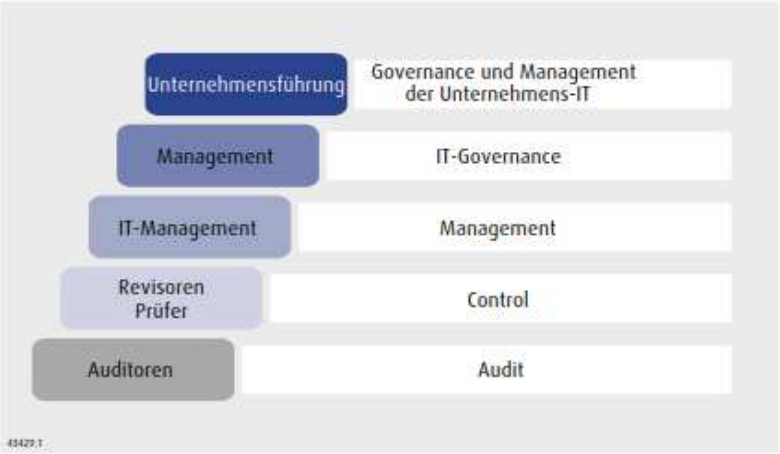

Bild 1. Fünf Stufen des Cobit-v5-Rahmenwerks der Governance in der Unternehmens-IT

ware. Ein naheliegendes Aufgabenfeld ist zunächst die Strukturierung der Dokumentation und der Dokumentenablage. Einige Anbieter unterstützen in diesem Umfeld auch die Dokumentenlenkung mit einer entsprechenden Statusverfolgung. Darauf aufbauend lässt sich mit entsprechenden Publikationsfunktionen eine Veröffentlichung der abgelegten Dokumente beispielsweise im Intranet des Unternehmens verwirklichen. Die Transparenz der Prozesse und der Inhalte der Managementsysteme wird dadurch gefördert.

Überprüfung kann sicherstellen, dass Maßnahmen für nicht mehr existente Risiken entfallen und neu auftretende Risiken identifiziert werden. Besonders der erstgenannte Fall, der Entfall obsolet gewordener Maßnahmen, kann in Verbindung mit der Effizienzsteigerung bei Prozessen zu sinkenden Kosten für den Betrieb des ISMS führen.

Außer dem Blick auf mögliche Optimierungsmaßnahmen sollte der Fokus zur Weiterentwicklung des ISMS auf zwei Hauptbereichen liegen: Der Einführung nicht normativer Anteile der ISO/IEC 2700x-Reihe und der Integration in andere Managementsysteme.

Die Grundlage für die Zertifizierung eines ISMS sind die in der ISO/IEC 27001 und ihrem Anhang A genannten Anforderungen. Darüber hinaus existieren ergänzen-

des ISMS zu richten, um eine zukunftsfähige Lösung auszuwählen.

Die Vorteile einer Softwareunterstützung liegen in erster Linie in der Sammlung und Konzentration von Informationen sowie in der Unterstützung, Überwachung und teilweisen Automatisierung der für ein ISMS notwendigen Prozesse. Damit können geeignete Anwendungen sowohl bei der Optimierung von ISMS-Prozessen als auch bei der Integration verschiedener Managementsysteme und ihrer Prozesse hilfreich sein.

Kernpunkte der Zusammenfassung liegen in der Integration der Verantwortung, Organisation und Ressourcen für die einzelnen Bereiche, sowie in der Zusammenführung der Erzeugung dokumentierter Informationen in eine einheitliche Struktur. Die Vorteile liegen in einer reduzierten Dokumentation – übergreifend gültige Abschnitte müssen nur einmal geschrieben und gepflegt werden –, einem reduzierten personellen Aufwand – je nach Unternehmensgröße können Verantwortungen, Prozesse und Organisation zusammengelegt werden – und einem reduzierten zeitlichen Aufwand – Schulungen und Audits können für übergreifend gültige Themen zusammengelegt werden.

Systemunterstützung

Der bisher behandelte Blick auf die Organisation und Methodik des ISMS sollte nach der Erstzertifizierung noch um das Aktionsfeld eines technischen Blickwinkels erweitert werden. Hier geht es vor allem um die Implementierung einer geeigneten Software.

Mehrere Aufgabenfelder sind geeignet für die Unterstützung durch eine Software. Außer der reinen Dokumentenablage ist die Unterstützung der Prozessabläufe ein weiteres Aufgabenfeld, in dem eine Software unterstützen kann. Hier liegt der Fokus auf einer Optimierung der Prozesse und einer Unterstützung bei der Durchführung und Dokumentation der in jedem Kontrollsystem vorgesehenen Kontrollen – zum Beispiel durch im System hinterlegte Zeitpläne für Kontrollen einschließlich Erinnerungsfunktionen und durch vorgefertigte Berichts-Templates zum Nachweis der Kontrollen. Darüber hinaus sind in einigen Anwendungen auch Funktionen für ein Business Continuity Management integriert, die den Anwendungsbereich des Systems ausweiten. Als Schnittstelle zwischen technischer Unterstützung auf der einen Seite und Methodik des ISMS auf der anderen Seite bieten einige Anbieter auch vorgefertigte Inhalte oder Leitfäden in ihren Anwendungen an. Diese können als Einführungshilfen auch bei Spezialthemen eingesetzt werden.

Aus der am Markt vorhandenen Auswahl der verschiedenen Anbieter ist je nach angestrebtem Einsatzfeld die geeignete Software auszuwählen. Wie bei jeder Softwareauswahl ist ein Blick auf die angestrebte künftige Entwicklungsrichtung

Fazit

Die Erstzertifizierung ist als Startschuss für die stete Weiterentwicklung des ISMS zu betrachten. Optimierung, Standardisierung und Integration stehen außer der Implementierung einer geeigneten Softwareunterstützung oben auf der Agenda.

Abschließend darf nicht vergessen werden, dass die Zertifizierung in regelmäßigen Abständen wiederholt werden muss. Auch die anstehenden Rezertifizierungen sind angemessen zu planen und vorzubereiten.

Andreas Woelke,
Senior Manager,
PKF Fasselt Consulting GmbH,
Duisburg

>> andreas.woelke@pkf-consulting.de

>> www.pkf-consulting.de