Datenschutz und QM sind artverwandt

Wie ISO 9001:2015 und ISO 27001 mit einem BPM-System bedient werden

In Zeiten wachsender Cyber-Kriminalität muss der Umgang mit Daten – also deren Verarbeitung, Übermittlung und Speicherung – geregelt werden. Insbesondere Unternehmen, die in einem sensiblen Umfeld agieren, müssen in puncto Informationssicherheit hohen Anforderungen genügen. Ein Schweizer Softwareanbieter für den Finanzsektor wurde nach ISO 27001 zertifiziert, Basis war die BPM-Software von AAC Infotray.

Roger Peduzzi

Im Finanzbereich ist ein konsequenter und sicherer Umgang mit Informationen und Daten von größter Bedeutung. Deshalb verfügt die ICR Informatik AG über ein effektives Instrumentarium, um IT-Risiken zu identifizieren, zu bewerten und die Wirksamkeit von risikomindernden Maßnahmen zu überwachen. Dieses basiert auf der ISO-Norm 27001, die Belange der Informationssicherheit regelt. Dank der dokumentierten Nachweise kann das IT-Unternehmen das Sicherheitsbestreben gegenüber Management und Kunden jederzeit belegen.

Das Softwarehaus mit Sitz in Risch-Rotkreuz entwickelt Softwarelösungen für Pensionskassen und Vermögensverwalter. Darunter Lösungen für die Versicherten- und Rentnerverwaltung, die Wertschriftenbuchhaltung und das Investment-Controlling, die Hypothekenverwaltung sowie

die revisionssichere und digitale Archivierung und das Dokumentenmanagement. Im Bereich Qualitätsmanagement setzt man seit 2007 die Software Limsophy BPM von der AAC Infotray AG ein. Die Software-Module sind einzeln oder als integrierte Gesamtlösung, als On-Premise-Lösung oder als Software as a Service (SaaS) erhältlich. Gerade die Tatsache, dass SaaS-Lösungen angeboten werden, war ein entscheidender Auslöser für das ISO-27001-Projekt.

Um den Forderungen hinsichtlich Informationssicherheit zu entsprechen, strebte die Unternehmensführung eine Zertifizierung nach ISO 27001 an. Die Anforderungen dieser Norm mussten in ein Managementsystem integriert werden, das einen normenneutralen Ansatz unterstützt. In der Implementierungsphase von ISO 27001 hat sich dann gezeigt, dass zusätzliche Anforderungen der Norm wie die Klassifizierung von Dokumenten oder das umfassendere Risikomanagement sowie das Tracking der Maßnahmen ebenfalls von Limsophy BPM abgedeckt werden können.

Dies war eine positive Erkenntnis: Die bestehenden Daten und Module aus dem ISO 9001-System können als Basis für das ISO-Zertifikat 27001 genutzt werden. Mit dem kontinuierlichen Ausbau der Dokumentenlenkung und dem umfassenden Risikomanagement in Limsophy BPM wird ICR Informatik den Anforderungen der Norm gerecht. Diese verlangt einerseits eine Klassifizierung von Informationen und andererseits ein umfassendes Risikomanagement.

Informationen klassifizieren und Risiken auswerten

Die meisten Unternehmen definieren zumindest ansatzweise, welche Dokumente und Informationen von welchen Mitarbeitern oder weiteren Personen gelesen oder bearbeitet werden dürfen. Meist geschieht dies über Schreib- und Leserechte auf File-Servern. Mit einem intelligenten Dokumentenmanagementsystem wie jenem von Limsophy BPM wird es dank der Zugriffssteuerung von Dokumenten auf Benutzerebene möglich, die Klassifizierung von Informationen zu unterstützen und damit zu mehr Informationssicherheit beizutragen.

ICR Informatik hat im Rahmen des Aufbaus seines ISMS (Information Security Management System) zusätzliche Prozesse, Richtlinien und Arbeitsanweisungen erstellt, Informationen klassifiziert und mithilfe von Limsophy BPM in das bestehende Managementhandbuch integriert. Dokumente wie Richtlinien und Arbeitsanweisungen stehen den Mitarbeitern als PDF zur Verfügung und sind unveränderbar.

Basierend auf dem IT-Grundschutz-Katalog des deutschen Bundesamts für Sicherheit und Informationstechnik (BSI) hat ICR Informatik zunächst die für das Unternehmen relevanten Risiken bezüglich der Informationssicherheit identifiziert. Anschließend wurden die Eintrittswahrscheinlichkeit sowie das potenzielle Schadensausmaß der Risiken ausgewertet. Zu jedem Risiko wurden Maßnahmen festgelegt, die als Q-Meldungen erfasst wurden. Diese risikovermindernden Maßnahmen wurden in zwei Kategorien (technische ›››

und organisatorische) unterteilt und zur Erledigung an die zuständigen Mitarbeiter übergeben.

Während der Umsetzung konnte der Fortschritt dieser Aktivitäten einfach überwacht und auf Knopfdruck aufgerufen werden. Nach ihrer Erledigung wurden die Wirksamkeit der Maßnahmen überprüft, die Q-Meldungen quittiert und die Werte für die Auswirkungen und die Eintretenswahrscheinlichkeiten entsprechend angepasst.

Eine jährliche Überprüfung der Risiken ist eine der Anforderungen für die Aufrechterhaltung der Zertifizierung.

Limsophy BPM bietet für die Klassifizierung von Dokumenten und für das Risikomanagement insbesondere folgende Möglichkeiten:

- Schreib- und/oder Leserechte auf Dokumente oder Informationen vergeben,
- geltende Dokumente den Mitarbeitern als PDF (unveränderbar) oder im Browser zur Verfügung stellen,
- Versionierung und Verwaltung der Ursprungsdateien (Word, Excel etc.),
- die lückenlose Rückverfolgung von Änderungen an einem Dokument per Audit-Trail,
- Rollen und Verantwortlichkeiten übersichtlich dokumentieren,
- Richtlinien und Vorgabedokumente sind mit den Prozessen verknüpft, sodass die Mitarbeiter bei der Ausführung ihrer Arbeit die jeweils geltenden notwendigen Vorgaben auf Klick zur Verfügung haben,
- mit der Erfassung von Q-Meldungen werden risikomindernde Maßnahmen festgehalten und den zuständigen Mitarbeitern zur Bearbeitung übergeben,
- Umsetzungsaktivitäten lückenlos überwachen,
- der Informationsbeauftragte erstellt mit wenigen Klicks die periodischen Auswertungen für die kontinuierliche Verbesserung,
- Risiken übersichtlich und aktuell darstellen und die Restrisiken dokumentieren.

Die Zertifizierung nach ISO 27001 wurde auf Anhieb erreicht. Nach dreitägigem Audit konnte ICR Informatik das Zertifikat entgegennehmen. Die Planung erfolgte mit dem Auditmodul von Limsophy BPM. Es unterstützt die Auditplanung und Dokumentation sowohl für interne als auch für externe Audits. Die zu prüfenden Prozesse und die darin involvierten Funktionen und Personen werden auf Knopfdruck über die geplanten Audits verteilt. Auditprogramm und Auditbericht werden automatisch über eine Dokumentenvorlage erstellt. Aus dem Audit können Abweichungen, Empfehlungen und Hinweise resultieren. Der Auditor verfasst einen Auditbericht, wo er Abweichungen, Empfehlungen und Hinweise aufführt. Diese Abweichungen, Empfehlungen und Hinweise werden anschließend als Q-Meldung erfasst.

Informationssicherheit mit ISO 27000

Die ISO 27000-Reihe umfasst Standards der IT-Sicherheit, die dem aktuellen Stand der Technik und des Rechts entsprechen. Wie die QM-Norm ISO 9001:2015 ist ISO 27001 gemäß der High Level Structure aufgebaut.
Bei der ISO-Norm 27001 steht die Informationssicherheit im Fokus. Sie ist weit weniger prozessorientiert gelagert, als dies im Qualitätsmanagement der Fall ist. Im Zentrum stehen die Klassifizierung von Informationen (z. B. bezüglich Vertraulichkeit und Verfügbarkeit), die Auswertung von Risiken in Zusammenhang mit Informationssicherheit sowie die Einhaltung von regulatorischen Anforderungen.

Nachhaltiger Erfolg mit starken Partnern

Um das ISO-27001-Projekt erfolgreich umsetzen zu können, hat ICR Informatik in einer ersten Phase mithilfe der Roth IT Management Consulting GmbH ein initiales Informationssicherheits-Assessment durchgeführt. Danach fand eine Risikoanalyse und -bewertung statt. Unter der Leitung des Beraters wurde das Managementsystem aufgebaut und in das bestehende ISO 9001-System integriert.

Die Consys AG als Implementierungspartner von AAC Infotray war in diesem anspruchsvollen Projekt Ansprechpartner für alle Fragen im Zusammenhang mit Limsophy BPM: Installation, Customizing, Anwenderschulung und Support. Gemeinsam können so die wachsenden Ansprüche an ein Managementsystem abgedeckt werden – für die Sicherheit der Unternehmen und der Kunden. ■

INFORMATION & SERVICE

KONTAKT ZUM ANWENDER

Roger Peduzzi
ICR Informatik AG
T +41 41 798 10 10
info@icr.ch

KONTAKT ZUM ANBIETER

AAC Infotray AG
T +41 52 260 31 31
info@infotray.com

QZ-ARCHIV

Diesen Beitrag finden Sie online:
www.qz-online.de/1302144