ISO 27001 in KMU effizient umsetzen

- **Riskmanagement, Mitarbeiter-Awareness, Synergie-Nutzung**
- **Starkes Signal für Vertrauen und ein Plus im Wettbewerb**
- **Vorteile für Euro-SOX und Sarbanes Oxley**

„ISO 27001 ist größenunabhängig anwendbar. Mittels Risikoanalyse ergibt sich der individuelle Handlungsbedarf. So profitieren kleinere Unternehmen von einem schlanken, effektiven System."

Erich Scheiber,
CIS-Geschäftsführung

Der Markt spricht eine klare Sprache: Nachweise für Informationssicherheit werden von immer mehr Kunden explizit gefordert. Wie sich der internationale Security-Standard ISO 27001 in kleinen und mittleren Unternehmen effizient umsetzen lässt, zeigen drei Fallbeispiele: Selected Services, Fabasoft und CQR Payment Solutions wurden erfolgreich nach ISO 27001 zertifiziert und berichten über ihren Weg von der Implementierung zum Zertifikat.
ISO 27001 ist größenunabhängig anwendbar: Mittels Risikoanalyse ergibt sich der individuelle Handlungsbedarf. So profitieren kleine und mittlere Unternehmen von einem schlanken, effektiven System.

Informationssicherheit wird von immer mehr Kunden explizit gefordert

Firmenprofil:
Der Provider für Online-Zahlungsverkehr CQR Payment Solutions mit 90 Mitarbeitern in Wien ist eine Tochter des führenden Online-Wettanbieters bwin. 27 verschiedene Zahlungsmethoden werden B2B-Kunden rund um den Globus als Outsourcing-Service zur Verfügung gestellt. Dabei garantiert CQR hochsichere Verbindungen zu Finanzinstituten und Online-Marktplätzen.

Im Interview:
Information Security Manager Oliver Eckel

- **Herr Eckel, was waren die Motive für Einführung von Informationssicherheit nach ISO 27001?**

„Wir wollten ein starkes Signal in Richtung Vertrauen setzen. Das Outsourcing des gesamten Zahlungsverkehrs ist **ein Vertrauensthema**. Mit dem ISO-27001-Zertifikat ist CQR ein Vorreiter in der Branche, was bei unseren Kunden sehr gut aufgenommen wird."

- **Waren definierte Prozesse vorhanden oder war dieser Schritt Neuland?**

„CQR hatte bereits Prozesse nach dem Branchenstandard ‚Payment Card Industry Certification' definiert. Die Anforderungen überschneiden sich inhaltlich mit jenen der ISO 27001, so dass wir **Synergien nutzen** konnten. Während PCI technisch ausgerichtet ist, profitieren wir durch ISO 27001 von der Security-Organisation, Awareness-Maßnahmen und von Security-Prozessen, die über Kreditkartendaten hinaus **sämtliche sensible Informationen** einbeziehen."

- **Welchen internen Nutzen zieht das Unternehmen aus ISO 27001?**

„Viele Prozesse waren bei CQR auch vor der ISO-27001-Zertifizierung schon definiert. Aber durch Implementierung des Informationssicherheits-Managementsystems (ISMS) wurde alles in eine **einheitliche Struktur** gebracht. Da wir ein dynamisches Unternehmen mit starkem Wachstum und ständigen Veränderungen – auch beim Mitarbeiterstand – sind, ist die gewonnene **Nachvollziehbarkeit von Handlungen** und Abläufen ein großer Vorteil. Vom neuen User bis zur neuen Software werden **alle Änderungsprozesse** durch Change und Configuration Management geregelt."

- **Welche Strategie haben Sie für Implementierung und Zertifizierung verfolgt?**

„Während der sechsmonatigen Implementierungsphase haben wir einen Berater zugezogen, um die Normanforderungen **korrekt zu interpretieren** und effizient umzusetzen. Zum Thema Riskmanagement hatten wir branchenbedingt Wissen im Haus. Zudem konnten wir die Security-Abteilung der Muttergesellschaft hinzuziehen. Das Zusammentragen der Dokumentation war harte Arbeit, dafür ist der **laufende Aufwand für den Betrieb** des ISMS jetzt minimal. Insgesamt bewerten wir die ISO-27001-Implementierung als Gewinn – es handelt sich um Anforderungen, die man früher oder später ohnehin umsetzen sollte. Nach diesen **positiven Erfahrungen** ist geplant, auch die Muttergesellschaft bwin mit mehreren tausend Servern zertifizieren zu lassen, um die internen Prozesse weiter zu verbessern."

„Die ISO-27001-Implementierung ist ein Gewinn – es handelt sich um Anforderungen, die man früher oder später ohnehin umsetzen sollte."

Welche Vorteile bringt ISO 27001 für die Einhaltung von Euro-SOX?

„Als Unternehmen im öffentlichen Interesse unterliegt CQR den Anforderungen der 8. EU-Richtlinie, die die **Einführung eines Internen Kontrollsystems** vorsieht. Die IT- und Informationssicherheitsaspekte von Euro-SOX können wir direkt aus ISO 27001 ableiten. Um IKS und Risikomanagementsystem auf ihre Wirksamkeit zu überprüfen, müssen Abschlussprüfer laut Artikel 26 der 8. EU-Richtlinie **„internationale Standards" als Maßstab** anwenden. Die Dokumentation der IT- und TK-Infrastruktur ist dabei ein wesentlicher Aspekt."

„Ein brisanter Punkt betrifft die Frage nach der **Verantwortlichkeit des Managements**. Ohne nachweisbare Dokumentation besteht eine persönliche Haftung des Managements und kann als Organisationsverschulden sanktioniert werden. Auch vor diesem Hintergrund kommt unserem ISMS nach **ISO 27001 eine zentrale Bedeutung** zu. Das Zertifikat einer akkreditierten Organisation wie die CIS entspricht einem staatlich anerkannten Dokument und bietet den Nachweis, dass die IT unseres Unternehmens internationalen Standards entspricht. Da die in Euro-SOX geforderte Dokumentationspflicht durch ein ISO-zertifiziertes und nachweislich gelebtes Managementsystem automatisch erfüllt wird, sind die Verantwortungsträger damit von einer persönlichen Haftung weitestgehend verschont."

Firmenprofil:
Die Fabasoft Gruppe ist Hersteller für Standardsoftware für Electronic Government und Content Applications. Die Produkte bilden den gesamten Lebenszyklus von Dokumenten rechtssicher und nachvollziehbar ab: von der Erfassung über die Bearbeitung und Archivierung bis zur regelbasierten Lösung. Mit 200 Mitarbeitern weltweit in Österreich, Deutschland, Schweiz, Italien und USA ist Fabasoft ein dynamisches Unternehmen.

Im Interview: Quality- und Information-Security-Manager Karen Daghofer

- **Frau Daghofer, was waren die Motive für die ISMS-Einführung nach ISO 27001?**

„Als Dienstleister halten wir sensible und geschäftsrelevante Daten von Kunden. Diese gilt es zu schützen – nachweisbar, mittels Zertifizierung. Vertrauliches Papier kann man im Tresor lagern. Für komplexen Datenschutz mit digitalen, analogen und mentalen Informationen – zentral, lokal, mobil und in den Köpfen der Mitarbeiter gespeichert – wirkt ISO 27001 wie ein Tresor. Ein **wirksames System mit Struktur** und Kontrollmechanismen. Das Zertifikat ist auch eine wichtige Grundlage für zukünftige Software-as-a-Service (SaaS) Dienstleistungen."

- **Welcher Bereich des Unternehmens wurde zertifiziert?**

„Zertifiziert wurde das Stammhaus in Linz mit 150 Mitarbeitern, wo Rechenzentrum und Softwareentwicklung zentral beheimatet sind. Es wird überlegt, die ISO-27001-Zertifizierung **auf andere Standorte auszuweiten**. Besonders interessant könnte das in den USA werden, da **Dienstleister von SOX-pflichtigen US-Unternehmen** selbst SOX-Audits durchführen müssen. Mit ISO 27001 ist der IT- und Security-relevante Teil von Sarbanes Oxley bereits abgedeckt."

- **Welche Wettbewerbsvorteile lukrieren Sie aus dem Zertifikat?**

„Wir setzen damit ein Zeichen und präsentieren das ISO-27001-Zertifikat auf unserer Homepage, **auf Kundenevents** und legen es **bei Ausschreibungen** bei. Die CIS als Zertifizierungsgesellschaft hat aufgrund ihrer profunden Expertise ein gutes Renommee in der Branche."

- **Waren definierte Prozesse vorhanden oder war dieser Schritt Neuland?**

„Wir sind konzernweit nach ISO 9001 zertifiziert und haben ISO 27001 integrieren können. Auch IT- und Security-Prozesse waren bereits definiert. Wir haben die Anforderungen der ISO 27001 großteils schon gelebt, daher war es **ein logischer Schritt**, dies mit einer Zertifizierung sichtbar zu machen. Wir konnten das gesamte System ohne Berater innerhalb von acht Monaten implementieren."

- **Welche Punkte mussten neu erarbeitet werden?**

„Dokumentation und Handbuch wurden verfeinert. Ein spannender Aspekt war die Mitarbeiter-Awareness, wobei unser Vorstand **durch Begeisterung und Engagement** für das Thema eine große Vorbildwirkung hat. Neue Mitarbeiter durchlaufen unsere Academy, wo Informationssicherheit ein fester Bestandteil geworden ist. Weiters wurde eine interne Security-Richtlinie mittels Newsletter an die Mitarbeiter gesendet. Dies hat stark **zu Diskussionen angeregt** und so half uns die Mundpropaganda bei der Awareness-Bildung.

„ISO 27001 wirkt wie ein ‚Tresor' für komplexen Datenschutz: mit digitalen, analogen und mentalen Informationen – zentral, lokal, mobil und in den Köpfen der Mitarbeiter gespeichert."

Zusätzlich haben wir im Frühstücksraum wechselnde Plakate mit Security Slogans wie „Gib Dieben keine Chance" oder **„Greif zum Hörer"** (um Vorfälle zu melden) aufgehängt. Und nicht zuletzt werden Artikel zu ISO 27001 immer öfter in unserem internen Wiki verfasst. So zum Beispiel zuletzt ein Eintrag über Festplattensicherung mit Querverweis auf die Norm."

- **Wie haben Sie Risikomanagement nach ISO 27001 umgesetzt?**

„Im Selbststudium mit Literatur und Internetrecherchen. Außerdem hatten wir durch die IS-Manager-Ausbildung der CIS entsprechende Unterlagen im Haus. Die große Herausforderung war, Risiken und **Maßnahmen zusammenzuführen**. Es galt, die vorhandenen „Puzzleteile" systematisch zu erfassen. Dadurch erhielten wir einen **wertvollen Gesamtüberblick** und konnten sicher sein, kein Risiko zu übersehen und keine Doubletten mitzutragen. Als sinnvoller Erstellungsprozess hat sich herauskristallisiert: Risiken schriftlich erfassen, diskutieren, kürzen. Dann erst Maßnahmen definieren. So verhindert man ein Überladen des Systems."

- **Welche Methode haben Sie für die Risikoanalyse verwendet?**

„Die qualitative Methode ALARP. Diese hat uns aufgrund ihres einfachen Ansatzes überzeugt. In der Formel ‚Eintrittswahrscheinlichkeit x Auswirkung = Risiko' werden keine monetären Werte eingesetzt, was bei **Imageschaden schwierig** wäre, sondern ‚Schulnoten'. Die Ergebnisse werden grafisch als Matrix nach dem Ampelsystem rot-grün-gelb dargestellt. Um die Maßnahmenwirksamkeit messen zu können, haben wir unser **strategisches Kennzahlensystem** direkt mit dem Risikomanagement verknüpft."

- **Haben Sie einen Tipp für die Implementierung von ISO 27001?**

„Zeitpuffer einplanen und immer wieder einen Schritt zurückzugehen, um das System als Ganzes zu betrachten. Die **Gratwanderung bewegt sich** zwischen: So viel wie notwendig, so wenig wie möglich. Ein überladenes System wird in der Praxis nicht gelebt. Das System muss schlank und effizient sein."

Firmenprofil:
Die Selected Services GmbH ist ein Saas-Spezialist im SAP-Umfeld mit über 50 Mitarbeitern am Stammsitz Wien sowie in München, Frankfurt, Stuttgart, Detroit und Singapur. Die ASP-Lösung (Application Service Providing) POOL4TOOL ist eine webbasierte Mietsoftware mit Modulen zur Prozessoptimierung in Einkauf/ SRM, Logistik/SCM, Entwicklung und Qualität.

Im Interview: Chief Technical Officer (CTO) Michael Rösch

- **Herr Rösch, was waren die Motive für die Einführung von Informationssicherheit nach ISO 27001?**

  „Informationssicherheit ist für uns als Anbieter webbasierter Mietsoftware ein Business Need und nicht nur **in der Automobilindustrie hochaktuell**. Einer unserer Kunden, ein großes Zulieferunternehmen, verlangte explizit eine Zertifizierung nach ISO 27001 – vorausschauend, während er selbst noch vor der Implementierung stand. "

- **Waren definierte Prozesse vorhanden oder war dieser Schritt Neuland?**

  „Die Implementierung gestaltete sich leichter und schneller als erwartet. Vor allem, weil wir aufgrund unserer Geschäftsbeziehung zu einem US-börsennotierten Unternehmen bereits SOX-konforme Prozesse im Hause hatten. Die **Anforderungen von ISO 27001 und Sarbanes Oxley** überschneiden sich inhaltlich, daher konnten wir die Implementierung der ISO 27001 direkt auf den bereits definierten Prozessen aufsetzen."

- **Welche Strategie haben Sie für Implementierung und Zertifizierung verfolgt?**

  „Zur effizienten Umsetzung des Standards haben wir einen Berater hinzugezogen: Die Analyse der Prozesse, das Überarbeiten der Dokumentation, die Durchführung einer Risikoanalyse sowie die Klassifizierung von Dokumenten haben wir mit externer Hilfe umgesetzt. So konnten wir die **Implementierung innerhalb eines halben Jahres** bewältigen. Zertifiziert wurde der gesamte Standort Wien mit Software-Entwicklung, Support und Administration.
  Als **Vorbereitung für das Zertifizierungsaudit** haben wir ein Stage Review der CIS in Anspruch genommen. Die Zertifizierung im ersten Anlauf zu erlangen, ist überaus wichtig für die Motivation der Mitarbeiter, die das System dauerhaft ‚leben' sollen."

- **Welchen internen Nutzen zieht das Unternehmen aus ISO 27001?**

  „Die lückenlose Dokumentation aller Prozesse schafft Transparenz für das gesamte Unternehmen. Heikle Fragen wie die Vorgehensweise beim Ausscheiden von Mitarbeitern sind damit klar geregelt. Durch das **Incident- und Change Management** im Rahmen der ISO 27001 haben wir unsere Support-Prozesse verbessert und sämtliche dahinterliegende Workflows sowie den Einsatz von Trouble Tickets optimiert. So profitieren wir von der **gesteigerten Effizienz und den klaren Abläufen**. Unsere Kunden spüren dies in Form kürzerer Reaktions- und Durchlaufzeiten bei der Anfragebearbeitung. Daher war es uns auch wichtig, die Einführung der ISO 27001 mit einem Zertifikat zu besiegeln, um die interne Optimierung unserer Prozesse auch für unsere Kunden sichtbar zu machen."

„Durch Incident- und Change Management nach ISO 27001 haben wir Support-Prozesse sowie den Einsatz von Trouble Tickets verbessert. Unsere Kunden spüren dies in Form kürzerer Anfragebearbeitung."

- **Und die Vorteile gegenüber dem Mitbewerb?**

  „Standardisierte Prozesse, anerkannt und geprüft durch die unabhängige Zertifizierungsorganisation CIS, sind ein handfester Wettbewerbsvorteil am Markt: Die **Nachfrage von Seiten unserer Kunden** nach einer ISO 27001-Zertifizierung ist im vergangenen Jahr deutlich gestiegen. Das Zertifikat vermittelt unseren Kunden die Sicherheit, einen verlässlichen Partner zu haben."

- **Wie haben Sie Risikomanagement nach ISO 27001 umgesetzt?**

  „Der Bereich Risikomanagement war Neuland für uns, so dass wir diesen Aspekt mit einem Berater als Coach umgesetzt haben. Die Schwerpunkte lagen dabei vor allem auf **Vertragsthemen, Haftungsfragen** und weiteren juristischen Belangen, denn Ausfallsicherheit war bereits durch die SOX-Anforderungen abgedeckt."

- **Ist auch eine ISO-20000-Zertifizierung geplant?**

  „Ja, diese ist in Planung. Und zwar als integriertes System mit ISO 27001, um Synergien im Betrieb bis hin zu Kombinationsaudits nutzen zu können. POOL4TOOL bildet bereits ITIL konforme Prozesse über das eigene Ticketing Modul ab. ISO 20000 ermöglicht es, die **ITIL-Konformität mittels Zertifikat** nachzuweisen. Daher streben wir eine Zertifizierung nach ISO 20000 an – ein weiterer Wettbewerbsvorsprung im internationalen Konkurrenzkampf."

Das Zertifikat macht Wettbewerbsvorsprung sichtbar

Von der Implementierung zum Zertifikat

- **Informationssicherheit nach ISO 27001**
- **IT-Service-Management nach ISO 20000**

Informationsgespräch
CIS-Erstgespräch: Details über Zertifizierungsprozess. Dann Registrierung, Projektplanung.

Analyse
Interne Evaluierung des Verbesserungspotentials, Bewertung vorhandener Maßnahmen.*

Implementierung
Maßnahmenumsetzung nach ISO 27001 und/oder ISO 20000 im Unternehmen.*

*Die CIS als unabhängige Prüfstelle ist nicht involviert

CIS Stage Review (Vorbeurteilung)
Optional: Projektbegleitende Prüfung der implementierten Elemente durch CIS-Auditoren.

CIS System & Risk Review (Vorbegutachtung)
CIS prüft Interpretation der Normforderungen und Dokumentation, „Generalprobe".

CIS Certification Audit
Überprüfung des Systems durch multiple Stichproben. Auditbericht mit zukünftigem Verbesserungspotenzial. Das CIS-Zertifikat nach ISO 27001 / ISO 20000 gilt 3 Jahre.

CIS Surveillance Audit
Das einmal pro Jahr durchgeführte Surveillance Audit überprüft die Effektivität des gesamten Managementsystems sowie seine ständige Verbesserung.

CIS Recertification Audit
Nach 3 Jahren haben Sie die Möglichkeit, das abgelaufene Zertifikat erfolgreich zu erneuern.

CIS - Certification & Information Security Services GmbH • A - 1010 Wien • Gonzagagasse 1/4/25 A • Tel: +43 (0)1 532 98 90, Fax: +43 (0)1 532 98 90 9 • E-Mail: office@cis-cert.com • Web: www.cis-cert.com