

## Kombinierte ISO 9001/BS 7799-2-Zertifizierung bei der atsec GmbH von Friedrich K. Abraham

Vor kurzem wurde die atsec information security GmbH erfolgreich offiziell gegen die Standards ISO/IEC 9001-2000 und BS 7799-2:2002 auditiert. Dies ist ein zweifacher Hinsicht ein beachtenswertes Ereignis. Zum einen gehört atsec zu den kleinsten Unternehmen, die je ein standardisiertes Managementsystem für Qualität und Informationssicherheit eingeführt haben und sich zudem der Prozedur eines formalen Audits unterzogen haben. Zum anderen handelt es sich um eines der ersten kombinierten Audits, die je durchgeführt wurden. In diesem White Paper werden die Motivation für dieses Projekt, die Herausforderungen und die Vorgehensweise beschrieben, um zu demonstrieren, dass solche Instrumentarien zur Steuerung auch für kleine Unternehmen hervorragend geeignet sind.

### Kurzdarstellung atsec / Ausgangslage

Die atsec information security GmbH ist ein Beratungsunternehmen, das sich ganz auf das Segment Informationssicherheit spezialisiert hat. Am Hauptsitz in München sowie in einem Büro in Köln sind derzeit gut 30 Mitarbeiter beschäftigt, bis auf wenige Ausnahmen Consultants. Das Geschäftsfeld lässt sich grob in zwei Bereiche gliedern, nämlich in das sicherheitsbezogene Projektgeschäft sowie in den Betrieb einer von Bundesamt für Sicherheit in der Informationstechnik (BSI) akkreditierten Common Criteria Prüfstelle.

Die Informationsverarbeitung lässt sich mit den Worten dezentral und heterogen kennzeichnen. Wie in nahezu jedem Unternehmen gibt es ein Intranet und die üblichen Back-Office-Applikationen. Die Berater jedoch sind in der Regel außer Haus tätig und das häufig weltweit. Ihre Ausrüstung ist auf mobiles Arbeiten ausgelegt, Notebook und Mobiltelefon sind ihre wesentlichen Elemente. Hardware und Applikationen müssen zudem die Anforderungen der verschiedensten Projekte bedienen. So benutzen atsecs Kunden beinahe jedes am Markt angebotene Workflow-System - und in die sind atsec-Mitarbeiter eingebunden. Das führt zu einer großen Vielfalt an eingesetzten Systemen unter den atsec-Mitarbeitern.

Die Anforderungen an Sicherheit und Qualität sind enorm. atsec hat in ihren Projekten Zugang zu hochsensiblen Informationen ihrer Kunden. Jede Verletzung der Wahrung der Vertraulichkeit hätte gravierende Auswirkungen auf den Geschäftserfolg. Zu den Prinzipien des Unternehmens gehören ein Höchstmaß an Integrität und Vertrauenswürdigkeit sowie der Anspruch, die höchste Qualität pünktlich zu liefern.

Es lag also auf der Hand, die Erreichung dieser Ziele durch die Implementierung eines Qualitäts- und Sicherheitsmanagements sicherzustellen. Die Anwendung der Standards ISO 9001 und BS 7799-2 für diese Zwecke lag ebenso nahe, denn sie sind in ihrem jeweiligen Segment „State-of-the-Art“. Die kritische Frage jedoch war, ob sich ein Unternehmen dieser geringen Größe die Einführung und den mit dauerhaften Kosten verbundenen Betrieb formaler Managementsysteme gemäß solch anspruchsvoller Standards überhaupt würde leisten können und ob sich diese Investition letztlich rechnen würde. atsec war davon überzeugt und entschloss sich daher, dieses ungewöhnliche Projekt anzugehen.

Zwei Gründe sprachen für die Machbarkeit des Projekts: zum einen waren wir überzeugt, Qualitäts- und Sicherheitsmanagement, wie es die beiden Standards fordern, faktisch bereits lange zu praktizieren, weshalb die Aufgabe hauptsächlich darin bestehen würde, die Dokumentation zu vervollständigen. Zum anderen sind wir der Ansicht, dass ein Unternehmen, dessen Geschäft Sicherheit ist, nur glaubwürdig sein kann, wenn es selbst mit gutem Beispiel vorangeht.

## Warum Zertifizierung?

Unabhängig von der Anwendung von Standards in einem Unternehmen stellte sich die Frage, ob ein externes Audit und eine formale Zertifizierung angestrebt werden sollten, denn beides ist nicht zwingend nötig.

Externe Audits sind ein Mittel der Qualitätssicherung, für das es keine echte Alternative gibt. Man kann zwar darüber diskutieren, wie häufig externe, unabhängige Prüfungen nötig sind, aber nicht darüber, ob sie sinnvoll sind.

Zertifikate sind immer zuerst ein Mittel der Außendarstellung. Auch atsec legt Wert darauf, in der Kommunikation mit Kunden und Partnern den eigenen hohen Standard hinsichtlich Qualität und Sicherheit auf diese Weise belegen zu können. Gerade für kleine Unternehmen kann ein Zertifikat das entscheidende Kriterium für den Erhalt eines Auftrags sein. Das trifft besonders zu, wenn der Geschäftspartner sehr groß ist und über eine Einkaufsabteilung verfügt. Vor allem in der Anfangsphase einer Zusammenarbeit legt dieser erfahrungsgemäß großen Wert auf die Erfüllung formaler Kriterien. Wenn nämlich geprüft wird, ob der Anbieter einer Dienstleistung oder Ware als Geschäftspartner in Frage kommt, hat der Einkäufer bei der Vielzahl geschäftlicher Kontakte, die er pflegen muss, oft gar keine andere Chance, als über formale Kriterien eine Vorauswahl zu treffen, ehe er sich Angebote im Detail ansieht. Ein Zertifikat garantiert zwar keinen Auftrag, doch umgekehrt kann sein Fehlen der Grund sein, dass man einen Auftrag nicht bekommt. Diese Erfahrung hat atsec selbst schon machen müssen - ein starkes Argument für eine Zertifizierung.

Und schließlich gab es noch einen Grund: Zertifizierungen gegen ISO 9001 sind eine recht alltägliche Angelegenheit und mittlerweile nimmt auch die Zahl der Zertifikate zu BS 7799-2 stetig zu - viele Unternehmen haben inzwischen beide Zertifikate erworben. Doch hatte man es je ausprobiert, beide Systeme gleichzeitig einzuführen, gemeinsam zu betreiben und auch gleichzeitig auditieren und zertifizieren zu lassen, um auf diese Weise den Aufwand zu reduzieren? atsec war kein solcher Fall bekannt, daher wollten wir die Durchführbarkeit dieses Vorhabens prüfen. Die Erkenntnisse aus einem solchen Projekt würden sich unmittelbar in atsecs Projektarbeit niederschlagen und als Erfahrung an unsere Kunden weitergegeben werden können.

## Strategie

Die meisten Mitarbeiter von atsec haben, ehe sie zu diesem Unternehmen kamen, in weit größeren Firmen gearbeitet - und dort einschlägige Erfahrungen mit dem Qualitätsmanagement machen müssen. Es überwog der Eindruck, dass Qualitätsmanagementsysteme nach ISO 9001 im Dienstleistungssektor oft nicht mehr sind als Potemkinsche Dörfer. Das Zertifikat ist die Fassade, die einen erschreckenden Mangel an Inhalt kaschiert. Und so mancher Geschäftsführer macht auch gar keinen Hehl daraus, dass es ihm eigentlich nur auf die Urkunde ankommt. Was sind die Gründe dafür?

Neben anderen Faktoren spielt nach unserer Auffassung eine bedeutende Rolle, dass ISO 9001 und mit ihm seine Befürworter immer wieder den Fehler begehen, sich selbst in den Mittelpunkt der Diskussion zu stellen. Der Standard fordert Prozesse, also werden alle Unternehmensabläufe in das Korsett formaler Prozesse gepresst. Der Standard fordert Dokumentation, also werden bergeweise Dokumente verfasst. Der Standard fordert organisatorische Maßnahmen, also werden Zuständigkeiten und Kompetenzen umgekrempelt. Das Resultat ist, dass sich bald der Eindruck verfestigt, dass das Qualitätsmanagement versucht, das Unternehmen nach seinen Vorstellungen umzugestalten. „Alles ist Qualitätsmanagement“, so ein authentisches Zitat eines QM-Auditors. Aber dieser Ansatz kann nicht funktionieren. Mancher mag das als besserwisserische Einmischung in seinen Verantwortungsbereich empfinden und steht dem skeptisch bis ablehnend gegenüber. Die Folge fehlender Unterstützung bei den Betroffenen ist dann, dass diese Managementsysteme letztlich nur aus einem Haufen Dokumente bestehen, die in staubigen Archiven lagern, ungelesen, unbenutzt. Und dem Zertifikat, stolz präsentiert in der Eingangshalle und auf der Website und bewacht von einem Qualitätsmanager, dem die Mittel fehlen, die ihm zugeordneten Aufgaben tatsächlich zu erfüllen.

Ein Unternehmen lebt nicht von Qualitätsmanagement oder Informationssicherheit, sondern von dem Ergebnis seiner Geschäftstätigkeit. Zu deren Durchführung gibt es Regeln, Verfahren und Methoden. Sie wurden geschaffen, damit die Arbeit effizient ist und hochwertige Ergebnisse liefert. Standards wie ISO 9001 und BS 7799-2 sollen dabei helfen, diese Regeln, Verfahren und Methoden zu implementieren. Wo sie das nicht können, sind sie überflüssig. Wo sie mehr wollen, überschreiten sie ihre Kompetenzen.

In diesem Bewusstsein gab es seitens der Geschäftsleitung eine klare Vorgabe an das Projektteam. Es galt, ein Managementsystem für die tägliche Anwendung im betrieblichen Alltag zu entwickeln. Nichts sollte eingeführt werden, nur weil es ein Standard fordert. Die essentiellen Abläufe des Unternehmens sollten optimiert werden und dabei waren die Anregungen und Forderungen von ISO 9001 und BS 7799-2 da, wo es sinnvoll war, zu beherzigen. Natürlich war klar, dass sich einiges ändern würde: Aufgaben, Abläufe, Zuständigkeiten, Technik. Ansonsten wäre das ganze Projekt auch überflüssig gewesen. Aber man wollte kein neues Unternehmen schaffen. Es funktionierte so, wie es war, gut. Alle Veränderungen mussten sich an der gelebten Praxis orientieren und dort, wo Dinge neu eingeführt oder vereinheitlicht werden sollten, waren nur Entwürfe akzeptabel, welche die Mitarbeiter mit einem Minimum an Formalismus und Regularien konfrontieren würden. Nur das würde nämlich Anlass zur Hoffnung geben, dass das ganze System im Alltag später auch angewendet werden würde, wenn erst einmal alle Sonntagsreden verklungen sein würden. Alles andere wäre mit dem eigenen Anspruch nicht vereinbar gewesen. Alles andere wäre auch letztlich wirtschaftlich auch gar nicht zu vertreten gewesen.

## Kulturelle Herausforderungen

Bei der Durchführung des Projektes galt es, mit einer ganzen Reihe von Herausforderungen fertig zu werden.

Es schien uns eine schwierige Aufgabe zu sein, in einem so heterogenen Umfeld, wie es bei atsec vorherrscht, Dinge zu formalisieren. Die sehr unterschiedlichen Projekte führen dazu, dass die Mitarbeiter für ihre Arbeit sehr verschiedene Hilfsmittel und Methoden nutzen. Wie aber können Steuerungsinstrumente aussehen, wenn sich wesentliche Parameter der Arbeit quasi täglich ändern? Wie definiert man Qualität, wenn die Arbeit eben nicht nach einem sich ständig wiederholenden Muster abläuft, sondern die Anforderungen der Kunden jedem einzelnen Mitarbeiter äußerste Kreativität abverlangt, was geradezu eine Absage an alles Prozessdenken zu sein scheint?

Neben solchen prinzipiellen Fragestellungen gab es auch ganz handfeste Herausforderungen. So kommen die Mitarbeiter der Firma aus rund zehn verschiedenen Ländern und damit Sprach- und Kulturräumen. Das führte zu intensiven Diskussionen, etwa zur Frage, in welcher Sprache welcher Teil der Dokumentation abzufassen sei, welche Auflagen ein Arbeitgeber seinen Mitarbeitern machen darf, machen muss oder auch umgekehrt nicht zu machen braucht, weil sie ohnehin selbstverständlich sind, und welche Prozeduren einzuhalten sind, wenn Regelungen verkündet und in Kraft gesetzt werden sollen. Richtlinien und Anweisungen zu verfassen ist einfach. Dafür zu sorgen, dass sie auch befolgt werden, kann aber zu einem unüberwindbaren Hindernis werden, wenn man sie an den kulturellen Besonderheiten des Unternehmens vorbei entwickelt, indem man zum Beispiel überreguliert oder praxisferne Vorgaben macht, die nur mit unangemessen hohem Aufwand umzusetzen sind.

Auch die Kunden von atsec sind in den verschiedensten Ländern ansässig. Die Begriffe aus dem Qualitäts- und Sicherheitsmanagement werden aber regional ganz unterschiedlich buchstabiert. Es war notwendig, Zielvorgaben zu spezifizieren, die den zum Teil sehr widersprüchlichen Vorstellungen Rechnung trugen, bis hin zu den Tücken einer lokalen Gesetzgebung. So musste zum Beispiel bei der Abfassung der Datenschutz-Policy beachtet werden, dass die Definition dessen, was personenbezogene Daten sind, von nationalen Gegebenheiten abhängt. atsec ist als deutsches Unternehmen sicher primär der deutschen bzw. europäischen Gesetzgebung unterworfen, doch atsecs Kunden bewerten ihren Partner eher mit Blick auf die eigenen, lokalen Regularien.

## Die Suche nach Partnern

Unerwartet schwierig gestaltete sich die Suche nach einem Zertifizierer. Unternehmen, die eine Zertifizierung gegen ISO 9001 anbieten, gibt es genügend. Bei BS 7799-2 ist die Auswahl kleiner, aber immer noch ausreichend. Das Problem lag nicht darin, ein Unternehmen zu finden, welches die Zertifizierung beider Standards beherrscht, sondern eine konkrete, einzelne Person als Partner zu gewinnen, die als gemeinsamer Auditor in Frage käme. Die Auswahl war überschaubar und die meisten der angebotenen Auditoren kamen aus dem Ausland. Es ist aber zu bedenken, dass die Zusammenarbeit mit einem Auditor üblicherweise langjährig ist. Vor diesem Hintergrund schien es nicht sinnvoll zu sein, einen Auditor von weit weg her einfliegen zu lassen. Schon die damit anfallenden Kosten wollten wir gerne vermeiden. Wenn man aber einen Auditor als Partner ansieht, der einem helfen soll, Standards richtig zu verstehen und anzuwenden, ist eine gewisse räumliche Nähe gerade in der Anlaufphase mehr als hilfreich.

Nicht viel anders sah es bei einer möglichen Unterstützung bei der Planung und Implementierung der Managementsysteme aus. Bei Fragen der Informationssicherheit und bezüglich BS 7799-2 gehört atsec selbst zu den tiefsten Kennern. Zu ISO 9001 war lediglich Basiswissen vorhanden. Das Hinzuziehen von entsprechenden Experten wurde erwogen, aber bald verworfen. Es war niemand zu finden, der mit gewissem Recht von sich hätte sagen können, dass er beide Standards wirklich gut kennt, und zwar nicht nur den Buchstaben nach, sondern aus dem betrieblichen Alltag. Das Wissen einschlägiger Beratungsunternehmen beschränkt sich entweder auf Qualitäts- oder auf Sicherheitsmanagement und von dem jeweils anderen System sind nur Grundkenntnisse vorhanden. Und eigentlich ist es noch schlimmer: nicht wenige, die sich gut mit ISO 9001 auskennen, sind völlig auf dieses Thema fixiert. Sie sehen die Unternehmenswelt ziemlich einseitig durch die QM-Brille und ordnen dem alles andere unter. Zwar sind ihnen die Standardtexte bestens vertraut, doch den Bezug zu den vielen anderen Aufgaben eines betrieblichen Alltags haben sie mehr oder weniger verloren. Damit war atsec aber nicht gedient. Wir entschieden uns daher, die Implementierung ohne externe Unterstützung zu wagen.

## Randbedingungen

Es galt, einige wichtige Randbedingungen zu beachten. atsec ist offiziell vom Bundesamt für Sicherheit in der Informationstechnik (BSI) als Prüfstelle für Evaluierungen nach Common Criteria zugelassen. Um diesen Status zu erreichen, mussten wir umfangreiche Voraussetzungen schaffen. Hierzu gehörte das Erfüllen der Anforderungen des Standards ISO 17025. Aus diesem lassen sich zahlreichen Einzelanforderungen ableiten, die sich teilweise mit den Forderungen von ISO 9001 und BSI 7799-2 decken. Prozesse und Dokumentation, die für die Prüfstelle entwickelt worden waren, mussten in das neue Managementsystem eingebunden werden, ohne spezifische Anforderungen von ISO 17025 zu verletzen, denn natürlich wollte atsec sich nicht zwei parallele Managementwelten leisten. Prüfstellen werden regelmäßig vom BSI daraufhin untersucht, ob sie die Anforderungen an solche Institutionen weiterhin erfüllen, also einmal implementierte Verfahren und Technologien weiterhin nutzen. Diese externen Audits galt es in das generelle Schema für Audits einzubinden, wie es von ISO 9001 und BS 7799-2 gefordert wird, um doppelte Prüfarbeit und eventuell widersprüchliche Prüfergebnisse zu vermeiden.

Zeitgleich mit dem Aufbau des Qualitäts- und Sicherheitsmanagements wollte atsec auch die Voraussetzungen schaffen, vom Bundeswirtschaftsministerium zum Umgang mit Verschlusssachen ermächtigt zu werden. Vorschriften und Sicherheitsmaßnahmen mussten entsprechend streng ausgelegt sein.

Schließlich galt es auch noch, ein vollständiges Datenschutzmanagement ins Leben zu rufen. Bislang hatte atsec nur die minimalen Forderungen der Datenschutzgesetzgebung erfüllt. Als Beratungsunternehmen für Informationssicherheit war unser Anspruch aber höher. Datenschutz sollte in einer Form praktiziert werden, wie es dem Geist der diesbezüglichen Regularien entspricht und außerdem neben den nationalen Einzelbestimmungen auch konkret die Ziele widerspiegeln, die der Datenschutz nach Buchstaben und Geist in den Ländern verfolgt, in denen atsec tätig ist.

## Planung

atsec begann das Projekt der Implementierung eines Qualitäts- und Sicherheitsmanagements mit einer Bestandsaufnahme. Wie sahen die Informations- und Kommunikationstechnik sowie die sie stützende Infrastruktur aus? Welche Qualitäts- und Sicherheitsziele hatte das Unternehmen? Welche Qualitätsmerkmale hatten die wesentlichen Geschäftsprozesse? Welche Sicherheitsbedarfe ließen sich daraus für die einzelnen IT-Assets formulieren? Welche Risiken gab es? Welche Sicherheitseinrichtungen gab es und welche Restrisiken wurden davon nicht abgedeckt? Welche der von den Standards geforderten Prozesse gab es und wie formal waren sie implementiert?

Die Antworten auf solche und ähnliche Fragen waren nicht überraschend. Die Defizite lagen vornehmlich in zwei Bereichen. Es gab einerseits einen Mangel an Dokumentation. Die meisten Dinge, die seitens eines Qualitäts- oder Sicherheitsmanagements gefordert werden, waren zwar vorhanden, aber nicht schriftlich festgehalten, weder als Architekturbeschreibungen für planende oder implementierende Aktivitäten noch im Bereich betrieblicher Prozeduren. Andererseits, und das war im Grunde eine Folge des gerade beschriebenen Mangels an Dokumentation, gab es bei Technik und Prozessen fast unbegrenzt viel Heterogenität. Und die Sonderwege und -lösungen, deren sich die Mitarbeiter zur Erfüllung einer Aufgabe bedienten, ließen sich nicht immer als projektbedingt oder Nutzung gewollter kreativer Freiräume erklären. An dieser Stelle ergab sich durch das Fehlen von formalen Vorgaben ein Effizienzverlust.

Bei der Definition der Arbeitspakete für die Implementierung konnte atsec auf die umfangreiche Erfahrung aus diversen Projekten zurückgreifen, in denen man Kunden zu einer Zertifizierung geführt hatte. Fachlich lag die größte Herausforderung darin, die Prozesse und Dokumente so zu planen, dass sie möglichst geringe Folgekosten bei der permanenten Pflege verursachen würden, und zwar ohne dass der Inhalt der Dokumente zu einer Ansammlung von Allgemeinplätzen würde. Die Lösung hieß Modularisierung, also die Aufteilung in viele kleine Dokumente, sowie die Verwendung von Templates, Formularen und Checklisten.

## Implementierung

Auf der Grundlage der Ergebnisse der Ist-Aufnahme wurde ein Projektplan entworfen. Die Unternehmensleitung interessierte sich dabei vor allem für die Frage, welche personellen Ressourcen benötigt würden. atsec war dabei insofern in einer privilegierten Lage, als die nötigen Qualifikationen im eigenen Haus verfügbar waren. Doch leider hatten die ausgewiesenen Experten nur wenig Zeit, da sie oft in mehrere zeitintensive Projekte eingebunden waren - sie von diesen Projekten abzuziehen hätte beträchtliche Einnahmefälle zur Folge gehabt und damit die Kosten des internen Implementierungsprojekts dramatisch erhöht.

Es war demzufolge offensichtlich, dass ein Großteil der Arbeit weniger erfahrenen Teammitgliedern zufallen würde, z.B. solchen, die gerade erst zum Unternehmen gestoßen waren und noch nicht in dem Umfang für externe Projektarbeit gebraucht wurden wie die Senior Consultants. Ebenso offensichtlich war es aber auch, dass ohne die Steuerung und den Rat versierter Fachleute eine erfolgreiche Projektdurchführung unwahrscheinlich sein würde. Man beschloss deshalb, für die Projektkoordination und zur Führung der Nachwuchskräfte zwei erfahrene Kollegen abzustellen. Sie sollten den Gesamtfortschritt überwachen, Vorgaben formulieren, Reviews vornehmen und abschließende Feinschliffarbeiten durchführen. Die übrigen Arbeiten, allem voran die zeitaufwändige Erstellung von Dokumentation, wurden denjenigen Personen übertragen, die jeweils freie Kapazitäten hatten. So konnten wir die kostenintensive Expertise zu ISO 9001 und BS 7799-2 auf strategische Aufgaben fokussieren und den Großteil der Arbeit von weniger spezialisierten Personen durchführen lassen. Dies hatte ganz nebenbei auch einen positiven Trainingseffekt.

Vorteilhaft war, dass es zwischen den im Projektplan aufgeführten Arbeitspaketen recht wenige Abhängigkeiten gab. Damit war es möglich, die Arbeit auf viele Schultern zu verteilen. Auch konnten wir mit wechselnden personellen Ressourcen arbeiten und so auf Mitarbeiter zurückzugreifen, die unvorhergesehen oder nur für eine begrenzte Zeitdauer verfügbar waren.

## Fazit

Die Implementierung des Projektes erfolgte termingerecht und ohne nennenswerte Probleme, obwohl kein Mitarbeiter ausschließlich oder wenigstens überwiegend mit diesem Projekt befasst war.

Fast alle Dokumente mussten wegen der Tragweite der darin gemachten Aussagen von der Geschäftsführung kontrolliert und formal akzeptiert werden. Das war mit signifikantem Aufwand verbunden, sowohl wegen der Menge der Arbeit als auch wegen der gebotenen Sorgfaltspflicht. Unsere Erfahrung lehrt, für Managementreviews angemessen viel Zeit vorzusehen.

Als wenig empfehlenswert erwies sich der anfangs gewählte Ansatz, die Fachkompetenz der Mitarbeiter dahingehend zu nutzen, dass Dokumente stets mehreren Personen zum Review gegeben wurden. Leider bewahrheitete sich das Sprichwort, dass viele Köche den Brei verderben. Es gab so viele Anmerkungen und Verbesserungsvorschläge, dass manche Auseinandersetzung über den besten Weg die ernste Gefahr barg, in endlosen Grundsatzdebatten steckenzubleiben. Bezeichnenderweise ging es dabei fast stets um eher unwichtige Details. Einige Dokumente durchliefen bis zu einem halben Dutzend Reviewzyklen. Das hätte auf Dauer dazu geführt, dass der Terminplan nicht hätte eingehalten werden können. Deshalb wurde die Qualitätskontrolle bald auf einen Fachkollegen und ein Mitglied der Geschäftsleitung sowie einen einzigen Reviewzyklus begrenzt.

Einige wenige Dokumente, wie zum Beispiel die Vorlagen für Vertraulichkeitsvereinbarungen, wurden einer Anwaltskanzlei zur Prüfung übergeben, um ihre juristische Belastbarkeit sicherzustellen. Auch das war mit mehreren Reviewzyklen verbunden und kostete relativ viel Zeit.

Bei den Maßnahmen zur Steigerung von Qualität und Sicherheit gab es den meisten Nachholbedarf im Backoffice-Bereich, z.B. bei der Verbesserung der kaufmännischen Prozesse und der Zusammenarbeit mit Kunden und Partnern. Die wertschöpfenden Prozesse, allem voran die Projektarbeit und die dafür eingesetzten Werkzeuge, war von Anfang an in einem gutem Zustand.

Das externe Audit, das wie üblich in zwei Phasen erfolgte, nämlich einer Überprüfung der Aktenlage und eine Verifikation der Pläne gegen die Wirklichkeit des betrieblichen Alltags, war auf Anhieb erfolgreich, und zwar ohne bedeutsame Anmerkung im Prüfbericht. Insbesondere gab es keine Nonkonformitäten.

Das Qualitäts- und Sicherheitsmanagement von atsec steht nunmehr vor seiner Bewährungsprobe, nämlich dem Einsatz im Alltag. Diese Situation dürfte wohl jedem IT-Leiter vertraut sein: eine Reihe von Mitarbeitern hat eine sehr eigene Einstellung zu Regelungen jedweder Art. Für manchen Informatiker scheint es eine Glaubensfrage zu sein, die eigene Kreativität als einzigen Ordnungsfaktor zu akzeptieren und die Kompetenz des Managements hinsichtlich der Steuerung von Aktivitäten per se in Frage zu stellen. Vorschriften werden geflissentlich ignoriert und als Begründung müssen Argumente wie Flexibilität, kurze Innovationszyklen, Projektdruck und ähnliches herhalten. Insofern ist klar, dass auch wir bei atsec versuchen müssen, langfristig die Kultur zu verändern. Das wird aber nur gelingen können, wenn die Managementsysteme lebensnah bleiben und die Unternehmensleitung gewillt ist, die Einhaltung von Regeln durchzusetzen.