

Projektbegleitung

Erfahrungsbericht bei der Rentenanstalt/Swiss Life

Die Deregulierungs- und Globalisierungsdynamik zwingt die Assekuranz und damit auch die Rentenanstalt/Swiss Life-Gruppe sowie das Konzernrevisorat, sich neu auszurichten. Im Anschluss an einen Benchmark wurden die Aufgaben prozess- und risiko-orientiert in einem neuen Reglement des Konzernrevisorates zusammengefasst und per 1.1.1999 in Kraft gesetzt. Im Prüfungsauftrag wurde u.a. Folgendes festgelegt: Im Rahmen der Projektbegleitung vergewissert sich das Konzernrevisorat, dass das Interne Kontrollsystem (IKS) in den Lösungskonzepten für neue Organisations- und Informatiksysteme in angemessener Weise berücksichtigt wird.

Projektbegleitung im Entwicklungsprozess

Mit der strategischen Neuausrichtung der Kernkompetenzen im Vorsorgemarkt, Finanz- und Riskmanagement sowie den Informatikvorhaben in den Bereichen Multi-Channel-Vertrieb und internationales Netzwerk gewinnt die konsequente Projektdurchführung an Bedeutung.

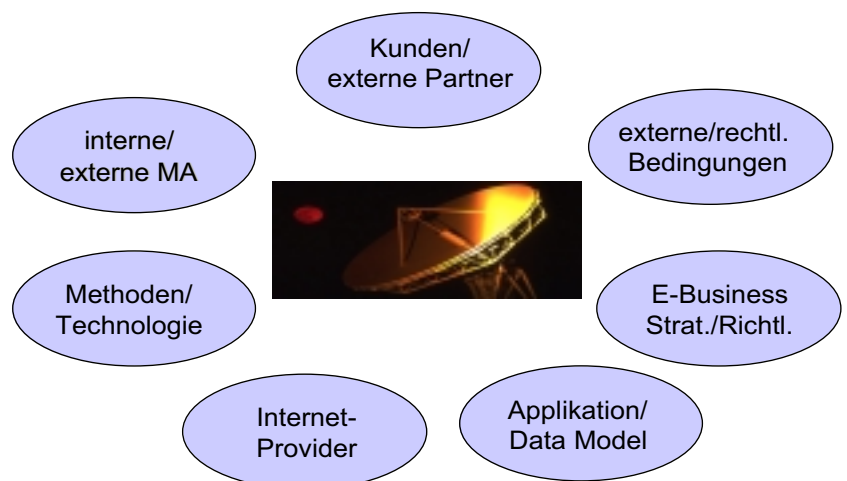
Die Prüfungsschwerpunkte der projektbegleitenden Revision bestehen einerseits aus dem Bereich der Projektabwicklung "Projektmanagement" und andererseits aus dem Bereich des zu entwickelnden Verfahrens "Anwendungssystem". Zur Gewährleistung

des IKS sind u.a. folgende Zielsetzungen zu erfüllen:

Beim Projektmanagement sind die Hauptziele Effektivität und Effizienz.

■ Spezifikationen – entspricht das System den Business-Anforderungen?

Einflussfaktoren bei E-Business-Projekten



■ Planung – sind Ressourcen vorhanden, um das Projekt zeitgerecht zu realisieren?

■ Budget – entsprechen Aufwand und Kosten den Vorgaben?

Bei den Anwendungssystemen sind die Hauptziele Vertraulichkeit, Integrität und Verfügbarkeit.

■ Recht – entspricht das System den rechtlichen Vorschriften?

■ Sicherheit – sind angemessene Konzepte und Verfahren vorhanden?

■ Qualität – ist die Ordnungsmässigkeit adäquat gewährleistet?

In der Vergangenheit haben wir uns bei der Projektbegleitung hauptsächlich auf den Einbau von angemessenen Kontrollen des zu entwickelnden Verfahrens konzentriert. Dadurch sollen schwerwiegende Risiken und finanzielle Verluste durch mangelnde Kontrollen nach der Einführung vermieden werden. Wir sind uns bewusst, dass die Sicherstellung des IKS während der Systementwicklung eine komplexe Aufgabe ist und von verschiedenen Einflussfaktoren abhängt.

Projektbegleitung ist Zusammenarbeit

Zu erwähnen ist, dass seit dem Aufbau der Informatikrevision im Jahre 1983 die projektbegleitende Revision am Hauptsitz der Rentenanstalt/Swiss Life praktiziert wird. Der Aufwand für die Projektbegleitung durch die Informatikrevisoren wird mit rund 30 % beziffert. Mit der zunehmenden Risiko- und Prozessorientierung kommt dem integrierten Approach sowohl bei den Systemprüfungen als auch bei der projektbegleitenden Revision immer mehr Bedeutung zu.

Die Aufgaben der Projektbegleitung gehen aus der nachstehenden Matrix hervor.

Funktionen- und Aufgabenmatrix des Konzernrevisorats					
Funktionen:	Beraten	Begutachten	Mitwirken	Prüfen	
Aufgaben:					
Stellungnahmen zu allen Phasenergebnissen					x
Einhaltung und Vollständigkeit der für das Projekt bestimmten internen und gesetzlichen Richtlinien und Weisungen		x		x	x
Erstellen von prozessbezogenen Risikoanalysen	x	x		x	
Beurteilen von Datenschutz und programmierten Sicherheitsvorkehrungen in allen Projektphasen	x	x		x	x
Beurteilen der Funktionentrennung und Einbau von organisatorischen Kontrollen und Abstimmungen	x	x		x	x
Richtigkeit und Vollständigkeit der Testkonzepte und Testresultate			x		x
Vollständigkeit der Genehmigung und der Dokumentation					x
Beurteilung des internen Kontrollsystems (IKS) und der Revisionsfähigkeit	x	x		x	x
Erstellung von Revisionskonzepten und Prüfprogrammen				x	x
Vollständigkeit der Qualitätssicherung und deren Massnahmen					x

Das heisst auch, dass Informatik- und Fachrevisoren immer enger zusammenarbeiten müssen. Natürlich gibt es noch viel voneinander zu lernen und Erfahrungen aufzubauen.

Gerade bei Internetprojekten ist die Projektbegleitung problematisch, weil alles sehr schnell gehen muss und nicht immer klar ist, wohin die Reise geht. Wir sind aber überzeugt, dass der eingeschlagene Weg – das gemeinsame Vorgehen – der Schlüssel zum Erfolg ist.

Kommunikation und Projektmanagement

Ohne die notwendige Kommunikation zwischen dem Informatik- und Linienmanagement bzw. der Projektleitung und dem Konzernrevisorat ist die Projektbegleitung zum Scheitern verurteilt. Schon früh hat das Konzernrevisorat die Kommunikationswege gesichert, damit die Phasenpapiere (vom Projektauftrag bis zum Abschlussbericht) an den verantwortlichen Informatikrevisor gelangen. Ebenso wurde die Mitarbeit des Konzernrevisorates im Projekthandbuch verankert.

Einsatz von Hilfsmitteln, Methoden und Verfahren

Im Rahmen der Projektbegleitung wurde bald festgestellt, dass die Projektleiter immer wieder nach Revisionsanforderungen fragten. Als Hilfsmittel wurde damals ein Leitfaden zur Gestaltung eines internen Kontrollsystems (IKS) bereitgestellt. Die Revisionskriterien wurden in drei Hauptgruppen dargestellt:

1. Aufbauorganisation (personenbezogen),
2. Ablauforganisation (informations- und anwendungsspezifisch),

3. Allgemeine Kriterien (Hardware- und Software-Technologie und Facilities).

Der Leitfaden steht heute allen Mitarbeitenden auf dem zentralen Informations-Server (ZIS) zur Verfügung.

Mit der Inkraftsetzung des COBIT Framework (Governance, Control and Audit for Information and related Technology), welches ab 2/1998 in der ganzen RA/SL-Gruppe als Standard gilt, beziehen wir uns bei der Projektbegleitung insbesondere auf die Kontrollziele der *Auslieferung und Unterstützung (AU1-13)*. Dieser Bereich – auch unter dem Begriff “applikatorische Kontrollen” bekannt – betrifft die Bereitstellung der gewünschten Dienstleistungen, welche vom traditionellen Betrieb über Sicherheits- und Kontinuitätsfragen bis zur Ausbildung reichen.

Mit dem Einsatz des COBIT Framework – übrigens seit 1/2000 in Deutsch verfügbar, www.isaca.ch – werden nun vermehrt Prüfungsschwerpunkte des Projektmanagements einbezogen, welche sich idealerweise mit den Kontrollzielen des Bereiches *Beschaffung und Einführung (BE1-6)* decken. Diese Ziele umfassen auch die Veränderungen und die Wartung von bestehenden Systemen. Die Prozesse der Projektabwicklung und die damit verbundenen Kontrollziele betreffen:

- BE1 Identifikation von Lösungen
- BE2 Beschaffung und Unterhalt von Anwendungssoftware
- BE3 Beschaffung und Unterhalt der technischen Infrastruktur
- BE4 Entwicklung und Unterhalt von Informatikverfahren
- BE5 Installation und Akkreditierung von Systemen

BE6 Änderungswesen

Im Bereich *E-Business* befasst sich die Informatikrevision der RA/SL mit weitergehenden Kontrollzielen, welche insbesondere bei den *E-Business*-Projekten in Betracht gezogen werden. Die Grundlage der ISACA unter dem Namen CONCT (Control Objectives for Net Centric Technology) wurde auf neue IT-Architekturen ausgerichtet und besteht aus vier Handbüchern zu den Themen:

- 1 CONCT Framework
- 2 Intranet/Extranet/Internet
- 3 Data Warehousing
- 4 Online Transaction Processing

Berichterstattung und Resultate

Entscheidend bei der Projektbegleitung sind kurz gehaltene Stellungnahmen, welche sich auf die Phasenergebnisse und -entscheidungen beziehen. Die Feststellungen sollten vor allem klar auf die erhaltenen Konzepte referenziert sein und angemessene Empfehlungen enthalten. Der Verteiler (u.a. Auftraggeber, Informatik, Fachbereich) ist so zu bestimmen, dass die Risiken erkannt und die empfohlenen Massnahmen bzw. Kontrollen eingebaut werden.

Mit der Projektbegleitung werden oftmals auch positive Nebeneffekte wie Sicherheitsbewusstsein, Verständnis für Kontrollen und Ausbildung bei den Betroffenen erzielt. Wichtig für die Revision ist aber auch der laufende Know-how-Transfer, welcher mit der Projektbegleitung “on the Job” gewährleistet wird.

Mit gut vorbereiteten Besprechungen und Gutachten sowie mit geschickten Verhandlungen lässt sich viel Zeit sparen. Nach dem Grundsatz “dienen und leisten”, d.h. mit einer zielgerichteten Dienstleistung, kann die Zusammenarbeit mit den Projektbeteiligten und vor allem die Akzeptanz des Revisors markant gesteigert werden.

Wir sind stolz auf die Mitarbeit und das Resultat der projektbegleitenden Revision in Bezug auf das Projekt SINAI (Sichere Internetanbindung). Die Mitwirkung betraf einerseits die Durchführung einer COBIT-basierten Risikoanalyse und andererseits die Erstellung eines Revisionskonzeptes. Die abgestimmten Grundlagen konnten bei der nachfolgenden Informatik-Systemprüfung sofort von der Revision eingesetzt und ergänzt werden.

Knowledge Management als Erfolgsfaktor

Erfolgreiches Knowledge Management in der Projektbegleitung kann sich nur einstellen, wenn der Wille vorherrscht, das Wissen zwischen Partnern zu teilen. Die Umsetzung verlangt ein soziales Umdenken und ein Streben nach guten Beziehungen und Kollegialität. Diese Elemente vereinfachen den Wissenstransfer und die Anwendung der Informationen zur Lösung des Problems.

Als Praxisbeispiel kann die Verbreitung der erwähnten Grundlagen angeführt werden, welche innerhalb und ausserhalb des Konzernrevisors, ja sogar länderübergreifend, übersetzt und verteilt wurden.



Bruno Wiederkehr und Nick Morgenthaler

Für die Gewährleistung eines effizienten Wissenstransfers können in Zukunft solche Informationen über das interne SL GroupNet von allen Mitarbeitenden der Rentenanstalt/Swiss Life-Gruppe bezogen werden.

Fazit

Aufgrund meiner bald 20-jährigen Erfahrung in der Projektbegleitung, den neuen Methoden und Verfahren sowie den vielschichtigen Einflussfaktoren bei *E-Business*-Applikationen kann ich bestätigen, dass sich die Projektbegleitung durch qualifizierte Revisoren geradezu aufdrängt. Der zunehmende Druck auf die Projektrealisierung verlangt vom Revisor nebst Kenntnissen der Informationstechnologie sowie der Rechts- und Finanzaspekte viel Erfahrung und Motivation, besonders aber Finger-spitzengefühl und Überzeugungskraft.

Ich bin überzeugt, dass mit einer ausgewogenen Projektbegleitung einerseits die Risiken von Anfang an vermindert und andererseits die Effektivität – *do the right things* – und die Effizienz – *do the things right* – gesteigert werden können.

Allen am Projekt Beteiligten muss bewusst gemacht werden, dass der Einsatz der projektbegleitenden Revision allein nicht für ausreichende Sicherheit und Kontrolle bürgen kann. Daraus lässt sich ableiten, dass die Verantwortung für ein qualitativ genügendes und wirtschaftlich gerechtfertigtes IKS den Verantwortlichen aller Stufen obliegt.

Konsequenz: Eine gute projektbegleitende Revision ist eine der Voraussetzungen für ein wirkungsvolles IKS.

Bruno Wiederkehr, Informatik-Revisor, Rentenanstalt/Swiss Life, Zürich

Résumé: L'accompagnement de projets à la Rentenanstalt/ Swiss Life

Depuis 1999, le nouveau règlement de la révision interne prévoit que celle-ci doit s'assurer dans le cadre de l'accompagnement des projets informatiques que les systèmes de contrôle interne adéquats sont intégrés dans les concepts des nouvelles applications informatiques.

Cette activité, qui mobilise environ 30% des ressources, se concentre sur deux tâches principales: (1) l'audit de la conduite des projets afin d'assurer l'efficacité et la rentabilité du développement informatique et la conformité aux buts stratégiques et (2) la vérification que les exigences en matière de sécurité, d'intégrité et de confidentialité sont respectées par les futures applications.

Les clés du succès résident dans:

- une information systématique du réviseur, qui reçoit pour information toutes les informations importantes relatives aux projets informatiques,
- l'établissement de normes, notamment un guide sur la manière de concevoir et d'implanter un système de contrôle interne, et la décision de donner à CobiT un caractère obligatoire pour toute l'entreprise,
- une communication des résultats des audits sous forme de brefs rapports contenant les constats et les recommandations correspondantes, adressés aux représentants des services utilisateurs et des services informatiques.

Cette démarche permet aux réviseurs de se tenir automatiquement au courant des développements technologiques. Elle exige cependant des réviseurs polyvalents, capables de maîtriser des domaines aussi variés que l'informatique, les finances, le droit et la gestion de projet, persuasifs et doués pour la communication.

Projektbegleitung

Wie ein Saulus zum Paulus wurde

Die Geschichte datiert über zwei Jahrzehnte zurück, hat meines Erachtens aber nichts an Aktualität bezüglich Projektmitarbeit des (Informatik-) Revisors eingeblüht.

Nach der Hayek-Reorganisation der SRG wurden diverse sogenannte Projekte initialisiert, welche die Organisation und die Administration der Rundfunk- und Fernsehanstalt neu ausrichten sollten. Eines davon (P2) befasste sich mit dem Rechnungswesen der Generaldirektion. Im Rahmen dieses Projektes durfte ich bei der Realisierung diverser Anwendungen und Programme als (externer) Systemberater mitwirken.

Ursprünglich aus der Zunft der Revisoren stammend, war es für mich als Leiter eines Teilprojektes "selbstverständlich", in der Projektorganisation die Unterstützung des Inspektorates vorzusehen. Leider meldete sich der erkorene Mitarbeiter für das Kick-Off-Meeting meines Projektes ferienhalber ab. An der ersten richtigen Projektsitzung fehlte er infolge Unpässlichkeit. Was das auch immer sein mag.

Die Projektgruppe hatte diverse grundsätzliche Fragen an das Inspektorat gehabt, die somit nicht besprochen werden konnten. Ich fasste sie schriftlich zusammen und sandte sie dem Inspektoratsmitarbeiter mit der Bitte, diese bis zur folgenden Sitzung der Projektgruppe zu bearbeiten.

Sie haben richtig getippt: Der Mitarbeiter erschien auch an der zweiten Sitzung nicht, "weil gerade mit einem Kassensturz im Tessin beschäftigt". Mein Hals war in der Zwischenzeit angeschwollen, so dass der Kragen am Platzen war. Ich ersuchte um eine Aussprache. Der nicht mehr ganz junge Revisor bequeme sich nach drei Anläufen meinerseits, mir relativ jungem "Schnösel" unter Beisein des Inspektoratsleiters Audienz zu gewähren.

Dabei kam zutage, dass es sich um ein "gebranntes Kind" handelte: Er war bei einem früheren Projekt einmal als "fünftes Rad am Wagen" dabei und stellte folgendes fest:

- Auf keine einzige seiner Forderungen bezüglich Ordnungsmässigkeit wurde eingetreten bzw. wenn entgegengenommen, im Projekt schliesslich nicht berücksichtigt.
- Diverse konstruktive Vorschläge wurden mit dem Hinweis zur Seite geschoben, "die Revision soll dann im nachhinein prüfen, ob das System genügend sei, und nicht im voraus motzen".
- Etliche seiner Bemerkungen wurden offensichtlich belächelt.
- Der Projektleiter gab ihm zu verstehen, er möge wohl ein guter Radiohörer (!) sein, verstehe von EDV jedoch nichts.
- Der Revisor sei heute zum Schluss gekommen, dass er tatsächlich die Sprache der EDV-Fritzen nicht beherrsche und er sich immer wieder mit technischen Ausdrücken konfrontiert

sehe, die ihm entgegengehalten würden und ihn überforderten.

Zusammenfassend glaube er, Projektmitarbeit der Revision sei eine Zeitverschwendung. Selbstverständlich war ich entsetzt über die Situation. Offensichtlich lag ein grosses Hindernis bezüglich Kommunikation vor.

Ich tat drei Dinge. Erstens entschuldigte ich mich in aller Form für das Verhalten des Teams, in welchem der Mitarbeiter "geschädigt" worden war. Dies, obschon weder ich noch sonst jemand aus meiner Firma am Unglück beteiligt gewesen waren. Zweitens gab ich dem Revisor zu verstehen, dass der Erfolg des Projektes wesentlich von seiner Unterstützung abhinge und die Projektgruppe auf seine Mitarbeit angewiesen wäre. Drittens fragte ich ihn, ob er gewillt wäre, probeweise für die nächsten zwei Projektsitzungen das Protokoll zu führen.

Ich sah zwei ungläubig blinzelnde Augenpaare auf mich gerichtet.

"Das ist doch eine Sache für eine Tippmamsel." "Ich weiss ja nicht genau, was protokolliert werden müsste." "Die EDV-Spezialausdrücke sagen mir doch nichts." Dies waren die ersten Reaktionen, die ich zu sehen und hören glaubte.

Ich spielte den Ball (oder war es ein Puck?) dem Inspektoratsleiter zu. "Sind Sie gleicher Meinung?" Auch nicht mehr der Jüngste, erkannte dieser aber die Situation goldrichtig: "Das wäre doch einen Versuch wert, und wir könnten von der Sache wahrscheinlich nur profitieren," war seine Schlussfolgerung. Mit guten Worten, das einem mit Keuchhusten darniederliegenden

Pferd auf die Beine geholfen hätte, gelang es dem Leiter, seinen Mitarbeiter zu einer Probeübung zu überzeugen. Ich versprach, bei der Beantwortung der schriftlich gestellten Fragen anlässlich einer Vorbesprechung behilflich zu sein, und die Protokollführung tatkräftig zu unterstützen.

Die nächste Sitzung war aus Sicht der Projektmitarbeiter eine Katastrophe:

- Die Beantwortung der vermeintlich einfachen Fragen warf eine ganze Reihe von Folgeproblemen auf, die von den Projektmitarbeitern offensichtlich nicht zu Ende gedacht worden waren.
- Die sich ergebenden Folgen könnten in Aufträge und letztlich in Arbeit ausarten.
- Der Protokollführer unterbrach immer wieder die Darlegungen der Sitzungsteilnehmer, um sich zu erkundigen, was nun protokolliert werden müsse und was gewisse Ausdrücke überhaupt bedeuteten.

Die Geduld der Projektmitarbeiter war derart strapaziert, dass einer meinte: “Wäre es nicht doch besser, man würde das Projekt in aller Ruhe abschliessen und dann könnte die Revision ja einfahren” (mit dem Hintergedanken, dass man dann ohnehin nichts mehr ändern könne). Ich stellte mich hinter “meinen” Protokollführer und gab der Meinung Ausdruck, wir hätten möglicherweise unsere Hausaufgaben nicht oder lausig gemacht. Denn wenn ein Aussenstehender nicht versteht, was vor sich geht, ist das Ganze offenbar nicht transparent genug beschrieben.

Murrend zog die Projektgruppe ab, sich schwörend, auf die nächste Sitzung besser vorbereitet zu sein, und

“es allen zu zeigen”. Zwischen dieser und der nächsten Sitzung des Projektteams fühlte ich mich wie zwischen Hammer und Amboss: Der Revisor glaubte, seine Befürchtungen bestätigt zu sehen (“ich habe es ja immer gesagt”), das Projektteam war sauer auf mich, weil ich diesem “Fossil” zu viel Beachtung schenkte.

Aber siehe da, die Mitglieder der Projektgruppe waren an der nächsten Sitzung plötzlich in der Lage, Sachverhalte ohne Turnübungen in Englisch und EDV-Kauderwelsch vorzutragen. Ich stellte zudem mit Verblüffung fest, dass sich der Revisor offenbar zwischen den beiden Sitzungen hinter EDV-Literatur geklemmt hatte und kompetent mit zu diskutieren begann! Es kam zwar immer wieder vor, dass er sich über Details aufklären lassen musste, weil er die Begriffe und deren Konsequenzen nicht auf den ersten Blick durchschaute. In der grossen Mehrzahl dieser Bitten um Erläuterungen mussten die Projektarbeiter aber (mit roten Ohren) gestehen, dass sie selbst “die Sache” nicht hundertprozentig durchdacht hatten und in Einzelfällen neue Ansätze zur Lösung von Problemen suchen mussten.

Auf diese Weise wuchsen in nur zwei Sitzungen gegenseitiger Respekt und eine echte Teamarbeit heran. Dem Revisor war plötzlich die Begeisterung an der Mitarbeit erwacht. Er gab mir am Ende seiner “Probezeit” zu verstehen, dass er *selbstverständlich* dabei bleiben wolle. Vielleicht lag es auch am Projekt (Kreditorenbuchhaltung) selbst, oder daran, dass ein Projektmitarbeiter an der zweiten Sitzung mit neuem Protokollführer Geburtstag hatte und alle zu einem Umtrunk einlud. Nach ein paar Glä-

sern waren alle mit dem Revisor per Du...

Bis zu seiner Pensionierung blieb der betreffende Revisor geschätztes Mitglied in diversen Projektgruppen. Heute hat sich in der SRG übrigens ergeben, dass ein ehemaliger Projektleiter zum Leiter des Inspektorats avancierte. Somit ist die Mitarbeit der Revision an wesentlichen Informatikprojekten nicht mehr wegzudenken. Insbesondere auch, weil ein ehemaliger Systemprogrammierer heute als CISA im Inspektorat der SRG tätig ist!

Max F. Bretscher, KPMG Fides Peat, Zürich

Résumé:

La conversion d'un réviseur

La question de l'accompagnement de projets informatiques par la révision a été le cadre d'une conversion épique, qui n'a rien perdu en actualité bien qu'elle date d'une vingtaine d'années.

Le réviseur interne de la TSR, convoqué en bonne et due forme par un nouveau chef de projet informatique, avait fait la sourde oreille et invoqué tous les prétextes pour ne pas s'intégrer au projet. Finalement contraint au dialogue, il expliqua que son attitude était le fruit d'un traumatisme lié à l'accompagnement d'un projet antérieur. Ridiculisé pour sa méconnaissance de la technologie, méprisé par les autres membres du projet, pas pris au sérieux et doutant finalement de ses propres compétences, il s'était juré de se tenir désormais à l'écart.

Finalement convaincu par le nouveau chef de projet de l'importance de sa

participation pour le succès du projet, il accepta de refaire une expérience. Le responsable de projet fit alors un pari risqué: confier durant deux séances la rédaction du procès-verbal au réviseur interne! Pari réussi, puisque cette méthode a contraint le réviseur à se faire expliquer toutes les questions techniques et le jargon informatique et les informaticiens a adopté un lan-

gage compréhensible pour des tiers et donc également pour les services utilisateurs.

Au terme des deux séances, un rapport de confiance fondé sur le respect mutuel était bâti et tout le monde se tutoyait. La collaboration de ce réviseur fut appréciée dans plusieurs autres projets jusqu'à l'heure de sa retraite.

permet de répondre à leurs attentes, de donner une image moins policière de l'audit et de créer une relation de partenariat avec ce département fédéral. Et puis, tant qu'à faire, si nous devons intervenir dans ce projet, autant le faire rapidement. Une intervention lors de la phase conceptuelle permet de mettre en place des solutions dont l'implantation après le passage en production n'est plus imaginable. Sur le plan des coûts également, plus le projet avance et moins les interventions de l'audit vont permettre de réaliser des économies. Un principe valable dans tous les projets, qu'il s'agisse de la construction d'un immeuble ou d'un projet informatique.

Projektbegleitung

Je persiste: un passage obligé mais un guêpier!

L'audit des projets informatiques durant leur développement est une des tâches les plus importantes mais également une des tâches les plus dangereuses de la révision.

Quelques conseils tirés d'expériences faites au sein de l'administration fédérale.

L'indispensable participation du réviseur

Dans la pratique, tout commence généralement de manière sympathique. Par exemple, une lettre cordiale qui invite un auditeur du Contrôle fédéral des finances à participer au projet d'introduction de SAP R/3 dans un département fédéral. Demande flatteuse qui montre que nos compétences sont reconnues. Un examen attentif de l'organisation de projet montre que le représentant de l'audit est membre à

part entière du groupe assurance-qualité, qu'il est à ce titre "responsable-qualité", doit établir le plan d'assurance-qualité et le plan de tests, doit définir les méthodes d'examen et les critères d'acceptation, qu'il doit participer à la surveillance des mesures prévues en matière d'assurance-qualité et qu'il doit enfin – en qualité d'examineur – examiner les résultats formellement et matériellement. Le tout en étant soumis à un chef de groupe qui ne dépend pas de l'audit.

De prime abord une demande parfaitement justifiée. La participation à ce projet permettra à notre réviseur de se former sur SAP R/3, de connaître ces applications et les nouveaux processus mis en place. Du *Knowledge-Management* à l'état pur... La nouvelle stratégie mise en place par le Contrôle fédéral des finances met l'accent sur la relation avec nos "clients" les offices fédéraux. Notre aide dans un tel projet

Stop!

Avant de se lancer donc tête baissée et souriante, il est encore temps et très nécessaire de se poser quelques questions.

Le principe d'indépendance de l'audit, implique que l'auditeur est indépendant dans le choix de ses priorités, dans l'établissement de son programme d'audit et finalement dans l'affectation de ses ressources. Pourquoi suivre ce projet et pas un autre qui se montre très discret? Comment savoir à quel moment de l'année des ressources seront nécessaires pour ce projet et éviter des collisions avec des audits planifiés? Comment évaluer le temps qui sera nécessaire à un tel accomplissement de projet?

A cet égard, deux constatations:

1. La fixation du calendrier de projet tout d'abord. Nous connaissons tous des exemples de projets dont le calendrier a été arrêté de la manière suivante. Première décision, généralement hautement politique ou stratégique: la date du passage en production. Pour plus de sûreté, cette date est bloquée par une communication officielle ou liée de manière définitive à un autre événement (déménagement, lancement d'un nouveau marché ou fusion d'entreprise). Puis vient le découpage: les phases du projet sont équitablement réparties entre la date du jour, pompeusement nommée *Kick-off-Meeting*, et la date-butoir fatidique. Et voilà le calendrier! C'était notamment le cas de la plupart des projets d'introduction d'applications appelées à remplacer les applications incompatibles avec l'an 2000, du projet d'introduction de la TVA et de bien d'autres encore. La réalité se chargera de vérifier la faisabilité de ce calendrier et placera l'auditeur devant le dilemme de devoir lâcher du lest sur ses exigences ou de se voir reproché d'avoir objectivement contribué à conduire le projet dans l'impasse.

2. Les phases que vous ne trouverez jamais dans un calendrier de projets. Par définition le temps est compté. Combien de projets prévoit-il une phase d'étude du rapport de fin de phase avant le passage à la phase suivante? Pourquoi dans la majorité des cas les documents de fin de phase doivent-ils être lus et approuvés en quelques heures? Quel calendrier prévoit-il après la phase de test une phase de correction des erreurs découvertes par

les tests? et une phase de test de la correction des erreurs?

Le problème, également classique, du profil de la personne idéale pour accompagner un projet est probablement insoluble. Il faudrait une personne que le jargon informatique ne rebute pas, qui maîtrise les processus de l'entreprise et les technologies actuelles, capable d'analyser un contrat et de se prononcer sur une analyse de rentabilité ou une question de protection des données, bref le mouton à cinq pattes. Le choix sera généralement dicté par les ressources disponibles et la mission exacte confiée à cette personne.

La mission? Probablement la question la plus centrale bien qu'elle soit ignorée par le Manuel suisse d'audit (MSA) qui n'aborde la question que sous l'angle de l'audit externe.

Selon le MSA, la mission de l'auditeur se fonde sur les critères de régularité au sens large, soit l'intégrité, la disponibilité, la conformité et la fiabilité des informations financières traitées par les applications informatiques. Cette définition exclu *de facto* l'accompagnement d'une application traitant des données non strictement financières, par exemple la gestion des dossiers médicaux des patients dans un hôpital ou celle des résultats de recherche d'un laboratoire chimique. Deux applications pourtant très sensibles et éventuellement essentielles à la survie de l'entreprise.

Second problème: qu'en est-il de l'audit de l'efficacité et de l'efficience? Comment un auditeur doit-il – ou peut-il – réagir en présence d'un projet remplissant ses exigences en matière de systèmes de contrôle internes ou de

trace d'audit mais qui n'est manifestement pas en accord avec les buts stratégiques de l'entreprise, ou qui fait double-emploi avec un autre projet, ou encore qui n'atteindra manifestement jamais la rentabilité promise lors de son initialisation? Pourra-t-il dégager sa responsabilité en invoquant une participation limitée aux critères de la régularité? Beaucoup de doutes, donc...

Et pourtant, il faut y aller!

Mais pas n'importe comment. Quatre règles de base qui ont fait leurs preuves:

Première règle: *édicter des directives contraignantes en matière de développement de projets*. En l'absence de règles obligatoires sur le plan national, le faire à l'échelon de l'entreprise, par exemple par un renvoi à COBIT. Il est essentiel de définir le cadre à respecter, pour permettre aux développeurs de l'intégrer dès le démarrage du projet.

Le Contrôle fédéral des finances a par exemple édicté en 1994 une directive sur les exigences minimales à observer dans le traitement des données financières (voir www.efk.admin.ch). Elles sont intégrées dans les directives distribuées aux comptables de l'administration fédérale et les chefs de projet informatique en reçoivent automatiquement un exemplaire dont ils doivent accuser réception. Elles renvoient notamment aux règles du Manuel suisse d'audit et aux normes de sécurité informatiques de l'administration.

Seconde règle: *identifier tous les projets et choisir les projets à accompagner en fonction de sa propre ana-*

lyse des risques. Les applications traitant les plus grands volumes financiers ne sont pas obligatoirement plus importantes que des application qui gèrent des processus indispensables à la survie de l'entreprise. Le moment et le type d'intervention dépendront dans une large mesure des risques identifiés. Il sera par exemple dans certains cas plus importants de vérifier l'intégrité des données reprises, plutôt que l'ergonomie des écrans ou la convivialité et les temps de réponse de l'application.

Ne pas oublier que chaque phase a ses risques. L'examen d'une phase d'étude se penchera sur les problèmes d'opportunité de la réalisation ou d'intégration dans la stratégie de l'entreprise, alors que la phase de paramétrisation sera le moment de vérifier que les traces d'audit sont activées de manière appropriée.

Troisième règle: *donner la priorité à une intervention de type audit plutôt qu'à une intégration dans une organisation de projet.* Cette démarche vous est plus familière et garantit que vos constats seront communiqués à vos partenaires traditionnels et ne disparaîtront pas dans une éphémère documentation de projet.

Le Contrôle fédéral des finances a fait de bonnes expériences avec des audits de phase de projet. L'examen en 1996 de la première phase d'introduction de SAP R/3 a par exemple permis les constats suivants (extrait du rapport d'activité 1996 du CDF):

L'examen de l'introduction des programmes SAP R/3 comme standard pour la comptabilité de l'administration fédérale a montré que le coût total

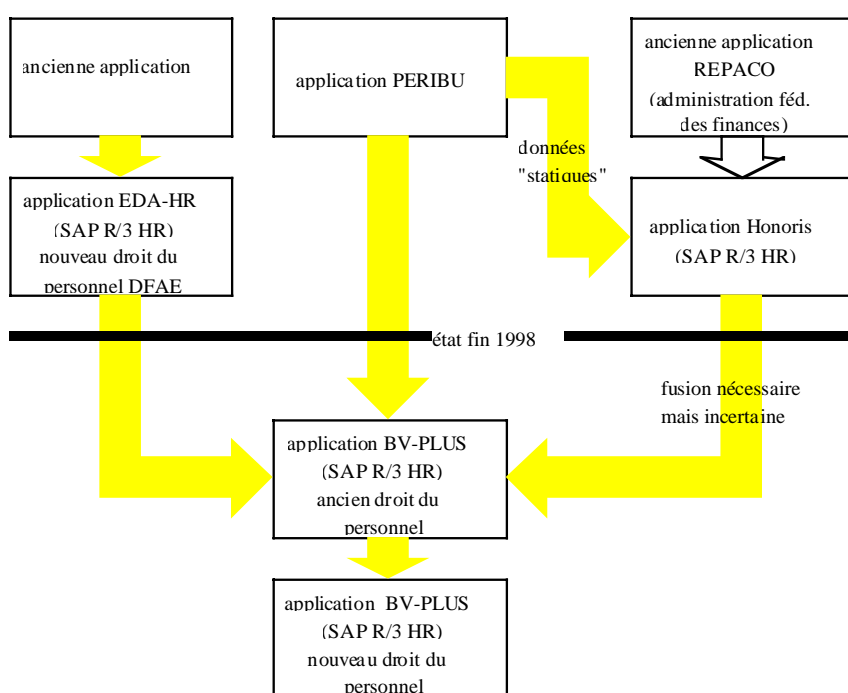
de ce projet n'avait pas été évalué. La Conférence informatique de la Confédération a pris la décision, en décembre 1994, sans attendre la fin du projet pilote, d'adopter le module financier de SAP R/3 comme standard pour les offices fédéraux. Par un effet de domino, de nombreux offices ont opté pour l'ensemble de la palette de modules SAP R/3, en adoptant les modules gérant notamment la facturation ou la logistique. Dans le domaine de la gestion du personnel fédéral, la récente réorientation du projet BV-PLUS conduira vraisemblablement au choix du module "Human Ressources" de SAP R/3. L'administration fédérale aura donc ainsi choisi une gamme complète de programmes sur la base d'un projet pilote qui ne portait que sur un seul module, n'était pas achevé, ne comportait aucun outil efficace de saisie des coûts et ne tenait pas compte du calcul de la rentabilité. L'examen du CDF a aussi montré que les exigences minimales en matière de sécurité et de fonctionnalité n'étaient pas encore

respectées, bien que divers services aient déjà utilisé ce programme en 1996.

L'examen dès la phase d'étude de l'intégration d'un projet dans l'entreprise et notamment ses relations avec d'autres projets "concurrents" permet de minimiser les risques (extrait du rapport d'activité 1998 du CDF).

Le CDF a examiné au courant de l'année 1998 trois projets développés avec le module HR (Human ressources) de SAP R/3, afin de s'assurer que les mesures nécessaires à leur intégration harmonieuse à terme dans une seule application avaient été prises. Il s'agit du projet du Département fédéral des affaires étrangères (EDA-HR), du projet BV-PLUS conduit par l'Office fédéral du personnel, ainsi que du projet Honoris de l'Administration fédérale des finances. Le schéma suivant illustre les liens entre ces différentes applications:

Liens entre les différents projets développés avec SAP R/3 HR



A l'occasion de l'audit informatique auprès du DFAE en 1998, le CDF a constaté qu'au stade actuel de développement, les mesures nécessaires à une intégration harmonieuse du projet EDA-HR dans le projet BV-PLUS avaient été prises.

Poursuivant ses examens, le CDF a en revanche constaté que l'intégration du projet Honoris (et vraisemblablement des autres projets développés sur le modèle "PINSAP") pourrait se révéler plus incertaine. Bien que ses différents interlocuteurs ne contestent pas la nécessité d'une telle intégration, le CDF n'a trouvé aucune description de celle-ci dans la documentation des différents projets.

La question de la définition de l'employeur est une question stratégique cruciale qui détermine d'une part le traitement des personnes travaillant dans deux offices et, d'autre part, le nombre et le "design" des liaisons avec les systèmes informatiques de la Caisse fédérale de compensation et de la Caisse fédérale de pensions (SUPIS). Ces questions ont été communiquées aux directions de projet respectives et le CDF suivra les réponses qui y seront apportées.

Quatrième règle: *intervenir de manière complète*. Il n'est pas judicieux de limiter par exemple l'examen aux questions de régularité en laissant de côté les questions de rentabilité. Mieux vaut examiner ou accompagner moins de projets mais le faire de manière complète. Le recours à un instrument comme CobiT permet d'assurer une démarche cohérente et complète.

Ne pas oublier que l'audit est également un utilisateur

Un des points qui justifie toujours une intervention dans un projet est la question des outils d'audit. Lors de l'établissement du cahier des charges de la future application, veillez à ce que le logiciel choisi offre des outils d'analyse de données qui répondent aux besoins de l'audit. Lors de la commande du logiciel et de son installation, assurez-vous que les options nécessaires ont été installées et activées. Testez ces outils et utilisez-les dans le cadre des tests de la nouvelle application.

Dernier conseil: soyez prudents!

Et n'oubliez pas votre fonction. La saine camaraderie au sein d'un projet est sympathique et contagieuse, mais les risques sont réels. Documentez vos observations et conservez vos notes de manière séparée. Et si vous voulez vraiment certifier quelque chose, ne certifiez que ce que vous avez vous-même contrôlé (attention aux erreurs ajoutées par des corrections successives) et avec les réserves d'usage. Voir à cet égard les bons conseils de la communication professionnelle numéro 9 sur la certification de logiciels.

Michel Huissoud, Contrôle fédéral des finances

Zusammenfassung: Ein notwendiger Weg, aber ein Wespennest!

Die eidg. Finanzkontrolle hat immer wieder die Möglichkeit, Informatikprojekte der Verwaltung des Bundes zu begleiten. Auf der einen Seite schmeichelt die jeweilige Aufforderung der Projektleitungen, sich an der Projektarbeit zu beteiligen, andererseits stellt sich immer wieder das Anliegen der Unabhängigkeit. Der Autor schliesst aus seinen Erfahrungen auf vier Regeln, die bei der Projektbegleitung zu beachten sind:

- Erlassen von zwingenden Weisungen zur Projektentwicklung. COBIT könnte ein Massstab sein.
- Vollständiges Projektinventar mit einschlägiger Risikoanalyse, die zu einer Priorisierung der Projekte bezüglich Projektbegleitung führt. Projekte des Rechnungswesens sind nicht zwangsläufig auch jene mit hoher Priorität!
- Die Beachtung der Revisionsaspekte ist höher einzustufen als die direkte Projektarbeit.
- Umfassende Betrachtung der Projekt- und Revisionsziele: Es genügt nicht, sich nur auf Ordnungsmässigkeitsaspekte zu beschränken und dabei Wirtschaftlichkeit und Wirksamkeit zu vergessen.

Der Autor stellt fest, dass der Revisor auch Benutzer des zu erstellenden Systems ist. Sein letzter Rat: Seid vorsichtig!

Projektbegleitung

Einbezug der Informatikrevision

(Auszug aus dem CISA-Prüfungsvorbereitungskurs 2000 von Peter R. Bitterli)

Die Praxis hat gezeigt, wie wichtig im Rahmen von Entwicklung und Unterhalt von Informatikprojekten der Beizug einer unabhängigen Stelle ist. Neben dem Projektcontrolling oder der Qualitätssicherung kommt dafür am ehesten die (projektbegleitende) Informatikrevision in Frage, wobei diese Aufgabe in den meisten Fällen nur von internen Stellen wahrgenommen werden kann.

Projektbegleitende Revision (Definition)

Die projektbegleitende Revision prüft eine Anwendung bereits während ihrer Entwicklung (ex ante).

Kriterien für Einbezug der Revision

Die (Informatik-)Revision kann aufgrund ihrer beschränkten Kapazität nicht sämtliche Informatikprojekte begleiten; sie muss daher die geplanten Projekte im Rahmen einer Risikoanalyse beurteilen. Die verfügbare Kapazität ist auf diejenigen Projekte mit dem grössten Projektrisiko zu verteilen.

Es gibt verschiedene mögliche Ansätze, die für die Revision "interessanten" Projekte zu finden. Einerseits kann dies mittels der Analyse der Projektmanagementrisiken erfolgen, welche weiter vorne beschrieben ist (z.B.

ab 25 Punkte: Revision liest und beurteilt die Phasenpapiere; ab 37 Punkte: Revision nimmt Einsitz in Arbeitsgruppe und versucht so, einen positiven Einfluss auf das Projektmanagementrisiko auszuüben). Eine andere Möglichkeit ist die Konzentration auf einige wenige, meist leichter messbaren Kriterien (siehe nächste Seite).

Mögliche Beurteilungskriterien sind beispielsweise der Entwicklungsaufwand in Tagen, Projektdauer und Projektkosten, die Bedeutung des Projektes für die Gesamtunternehmung,

die erwartete Komplexität, die eigentlichen Projektrisiken sowie die erwartete Intensität für am Projekt beteiligte Personen. Die genaue Bedeutung der erwähnten Kriterien kann der Abbildung 1 entnommen werden.

Zeitpunkt der projektbegleitenden Revision

Die (Informatik-)Revision kann Projekte grundsätzlich zu jedem Zeitpunkt resp. in jeder Projektphase überprüfen. Erfahrungsgemäss ist ein Einsatz der Revision in einer sehr frühen Phase sinnvoll (Projektauftrag, Vorstudie, evt. Konzept) und dann wieder im Rahmen der Abnahme oder kurz danach. Da jedoch eine späte Korrektur von Fehlern (z.B. fehlende Prüfspur) nach der Implementierung ein Vielfaches von dem kostet, was man

Kriterien für Einbezug der Revision *

Projektumfang	Anzahl Personentage, Anzahl beteiligte Personen, Anzahl involvierte Fachbereiche
Projektdauer	Dauer des gesamten Projektes von der Initialisierung bis zur offiziellen Projektabnahme
Projektspezialitäten	Innovationsgrad, vorhandene/nicht vorhandene Erfahrungswerte, spezielle Infrastruktur, spezielle Methoden, besondere Vertragsbedingungen
Projektbedeutung	Einfluss auf den Unternehmensgewinn, Stellenwert gegenüber Konkurrenz, strategische Gewichtung für das Unternehmen
Projektkomplexität	gegenseitige Abhängigkeiten, Anzahl beteiligter Organisationseinheiten, Querverbindungen zu anderen (Teil-)Projekten
Projektkosten	alle Entwicklungs- und Managementkosten sowie alle Produktinvestitionskosten
Projektrisiken	möglicher Schaden, falls Projektziele nicht erreicht werden
Projektintensität	Überlastung, Auslastung oder Unterbeschäftigung der Mitarbeiter

*Die aufgeführten Kriterien sind Projektmerkmale nach "Organisationslehre für Wirtschaftsinformatiker"; Lehner et al.

Abbildung 1

dafür in einer der ersten Phasen aufwenden müsste, ist eine Beteiligung vorwiegend in den frühen Projektphasen vorzuziehen.

	Beurteilung der Anwendung	Beurteilung der Entwicklungsumgebung
während der Entwicklung	(eigentliche) projektbegleitende Revision	Prüfung von Methoden & Standards der Systementwicklung
bei der Abnahme	Software-Zertifizierung	Prüfung von Test- und Abnahmeverfahren
während dem Betrieb	applikationsabhängige Prüfung	Prüfung von Methoden & Standards der Wartung

Unterschiedliche Grade der Beteiligung der Revision

Der Grad der Involvierung in einem Projekt kann für den Informatikrevisor höchst unterschiedlich sein: von Stellungnahmen zu Phasenpapieren bis zur aktiven Mitarbeit in Teilprojekten als volles Mitglied der Projektgruppe. Dies kann jedoch die Unabhängigkeit der Revision an sich resp. des Revisionsmitarbeiters gefährden.

Ziele der projektbegleitenden Prüfung

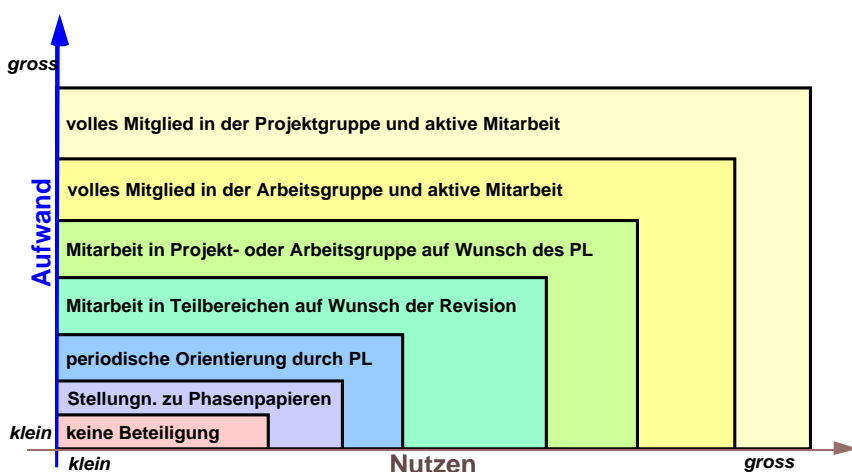
Die projektbegleitende Prüfung hat dieselben Ziele wie die konventionelle Revision: Ordnungsmässigkeit (IKS, Überwachung/Nachprüfbarkeit, Gesetzeskonformität, Dokumentation), Wirtschaftlichkeit (Effizienz, Projektorganisation) und der Sicherheit einer Anwendung im Rahmen der Informationstechnologie.

Risiken der projektbegleitenden Prüfung

- Revisionstätigkeit wird durch Management nicht unterstützt
- Revision wird durch Projektteam nicht akzeptiert
- Revision übernimmt operationelle Tätigkeiten
- Revision prüft ein System, das sie mitentwickelt hat (verliert Unabhängigkeit)
- Das Management verlässt sich zu sehr auf Revision
- Revision wird in Expertenstreit involviert

Nutzen der projektbegleitenden Prüfung

- Beitrag zur Qualität der Software
- rechtzeitige Berücksichtigung von Sicherheit/Kontrolle (Beratung/Schulung)
- Verminderung des Unternehmerisikos



Ergebnisse und Revisionsaufgaben bei der Informatik-Systementwicklung *

	1. Phase Vorstudie	2. Phase Konzept	3. Phase Detailfestlegung	4. Phase Programmierung und Test	5. Phase Systemtest und Einführung
Aktivitäten, Arbeitsergebnisse bei der Systemgestaltung	Ausarbeitung des Problemkatalogs Formulierung der Zielsetzungen und Systemanforderungen Grobanalyse der Lösungsmöglichkeiten Strukturierung des Gesamtsystems in Teilsysteme Analyse der Ressourcen Wirtschaftlichkeits- betrachtung	Ausarbeitung einer Gesamtkonzeption Evaluation der Lösungsvarianten Entwicklung einer integrierten Datenbasis Ressourcenplanung Strukturierung des Gesamtsystems Wirtschaftlichkeits- analyse	Detaillierung und Konkretisierung des Gesamtkonzeptes Darstellung des Informationsflusses Organisation und Sicherstellung des Datenmanagements Definition der Prüf- und Sicherheitsvorkehrungen Festlegung der Ressourcen Detaillierte Wirtschaft- lichkeitsanalyse	Ermittlung der Programmstruktur Programmerstellung Erstellen der Job Control Aufbau der Testorganisation Anpassung der Organisationsstrukturen Vorbereitung der Benutzerschulung Datenübernahme	Durchführung des Abnahmetests Überarbeitung der Benutzerdokumentation Leistung von Einfüh- rungsunterstützung Umstellung und Über- gabe des Systems
Aufgaben der Revision im Systementwicklungs- prozess	Überprüfung der Ist- Zustandsanalyse Beratung, Hinweise bei Organisationsproblemen Sammlung von Projektinformationen Überprüfung der Wirtschaftlichkeits- betrachtung	Formulierung der Anforderungen an das IKS Integration des IKS in das Gesamtsystem Einbau von Revisionshilfen Formulierung der Revisionsanforderungen für Kriterienkatalog des Evaluationsprozederes Prüfung und Kontrolle der Datenadministration Überprüfung der Wirt- schaftlichkeitsanalyse	Konsolidierung der Revisionsanforderungen durch Überwachung der Systemspezifikationen Konkretisierung und Sicherstellung der organisatorischen und programmtechnischen Kontrolle Überprüfung des Datenmanagements Sicherstellung der Prüfspur in den Verfahrensabläufen	Überprüfung der Systemspezifikationen auf Programmebene Prüfung der Revisionsfähigkeit der Programme Überwachung der Benutzerschulung Teilnahme bei Programm- und Systemtests	Prüfung der Test- organisation und des Testkonzepts Teilnahme bei Programm- und Systemtests Überprüfung der programmtechnischen und organisatorischen Kontrollen im Abnahme- test Beurteilung der Effizienz der IKS-Benutzer- schulung

* aus "Berücksichtigung der Revisionsanforderungen in der EDV-Systementwicklung"; Bruno Gloor

Peter R. Bitterli, Bitterli Consulting, Zürich

Projektbegleitung

Table ronde

Séminaire du 23 mai 2000 Quelques échos de la table ronde

Les questions sur lesquelles tout le monde est d'accord:

- la révision a un rôle essentiel à jouer dans le développement informatique,

- les exigences à remplir doivent être communiquées aussi rapidement que possible aux projets informatiques,
- il est à cet égard faux de parler des "exigences de la révision" car il s'agit en réalité des "exigences de la régularité" au sens du Code des Obligations. Ces exigences devraient d'abord être celles du propriétaire des données, soit par exemple le comptable de l'entreprise qui doit exiger que ses données

soient traitées correctement par la future application, et non celles du réviseur,

- les exigences en matière de régularité doivent dès leur formulation être traduites en cas à tester, intégrés immédiatement dans les plans de tests,
- trois paramètres sont intimement liés dans un projet: les délais, les coûts et les prestations. Beaucoup de projets informatiques échouent car des changements sont apportés de manière inconséquente à un seul de ces trois paramètres (les prestations en général) en oubliant d'adapter les deux autres.
- le réviseur ne doit pas maîtriser toutes les technologies informatiques

(cf l'article de J. Duffy, partenaire PWC, paru dans l'édition de février 1999 de *Internal Auditor*: "Trying to become a technology expert probably isn't the most effective use of an auditor's resources.").

Les points qui méritent l'attention des organes compétents de la Chambre fiduciaire:

- un effort devrait être consenti pour sensibiliser les services d'audit interne et mettre à leur disposition des outils adéquats (voir points suivants),
- l'absence sur le plan suisse d'une norme contraignante qui fixe les exigences minimales à observer dans le traitement informatique de données financières, notamment les exigences minimales en matière de systèmes de contrôle interne, de trace d'audit,
- la nécessité de traiter dans le Manuel suisse d'audit la question de l'accompagnement de projet en retenant également la mission de l'audit interne et les critères de rentabilité, d'efficacité et de confidentialité,
- la communication professionnelle no 13 traitant de l'EDI est utilisable comme norme, bien que sa formulation soit parfois trop vague. Elle peut constituer une bonne base pour une norme sur l'e-commerce.

Seminar vom 23. Mai 2000 Rosinen aus dem Gespräch am runden Tisch

Darüber ist sich jedermann einig:

- Die Revision spielt bei der Informatik-Projektentwicklung eine wichtige Rolle.
- Anforderungen sind so schnell wie möglich der Projektleitung mitzuteilen.



- Es ist in diesem Zusammenhang falsch, von Revisions-Anforderungen zu sprechen, weil es sich um Forderungen der Ordnungsmässigkeit im Sinne des Obligationenrechtes handelt. Demnach handelt es sich um Forderungen des Daten- und Anwendungsbesitzers (*data/application owner*) und nicht des Revisors.
- Ordnungsmässigkeitsanforderungen sind in den Testspielen und -plänen aufzunehmen.
- Drei Parameter sind in der Projektarbeit eng verknüpft: Termine, Kosten und Lösung. Es kommt (zu) oft vor, dass Änderungen an einem Parameter (meistens bei den Lösungsanforderungen) keine Berücksichtigung bei den andern beiden finden.
- Der Revisor muss nicht die gesamte Informationstechnologie beherrschen (siehe Artikel J. Duffy (Partner PwC) in der Februarausgabe 1999 des *Internal Auditor*: "Trying to become a technology expert probably isn't the most effective use of an auditor's resources.").

Punkte, welche die Aufmerksamkeit der zuständigen Stellen der Treuhandkammer verdienen:

- Es sollten Anstrengungen unternommen werden, um die internen Revisoren bezüglich projektbegleitender Revision besser zu unterstützen und ihnen Instrumente zur Verfügung zu stellen (siehe auch nachstehende Punkte).
- Es fehlen zwingende Weisungen oder Richtlinien, welche das Minimum bezüglich Interner Kontrolle und Prüfpfad im Umfeld von Informatikanwendungen beschreiben.
- Es besteht die Notwendigkeit, im Wirtschaftsprüferhandbuch (HWP) explizit und ausgedehnt auf die Projektbegleitung einzutreten, wobei auch wesentliche Anliegen der Internen Revision zu Worte kommen, wie Wirtschaftlichkeit, Vertraulichkeit, Wirksamkeit.
- Die Fachmitteilung Nr. 13 der Treuhandkammer bezüglich *Electronic Data Interchange* ist als Basis für Revisionen im Umfeld des *E-Commerce* brauchbar, obschon sie in einzelnen Teilen wenig präzise wirkt.