Managing Expectations with Service Level Agreements (SLA)

Outsourcing

Many organisations are examining their operations in order to identify where they should be focusing their management efforts and what are peripheral activities. These peripheral, or non core, activities only exist to support the main task of providing goods and services to the customer. As such they generally demand a disproportionate amount of management time and effort and often are undertaken in an inefficient manner, lacking as they do the economies of scale and the benefit of the latest best practices.

In addition, many businesses nowadays are confronted with increasing complexity of their business tasks and must deal with an increasingly interconnected environment. Various interest groups generating additional pressures by raising demands and expectations such as

- Raising performance and quality standards
- Intensifying customer relations and services
- Reducing costs and increasing profitability
- Shortening time-to-market

Companies can often not fulfil these demands and expectations prior to implementing major changes. In such situations, outsourcing is often considered to be an opportunity to reduce costs and release management efforts.

Integrated Approach

Whilst outsourcing is often considered to be an opportunity to reduce costs and release management efforts, these aims are not always the main result. Such exercises force a careful examination of the activities under consideration, questioning the need for the continuation of all the services enjoyed in the past and the levels of service really needed against each activity for the effective running of the business. Outsourcing forces a careful examination of the service in question which can often lead to a re-engineering of that function and also the way in which other business functions interact with it. As a result more appropriate services are defined and more efficient business practices begin to spread to other functions within the business.

One approach to achieve this goal is to implement a management environment according to the ISO 9000 framework. The heart of the ISO 9000 system philosophy is – as depicted in Figure 1 – to document what to do, do what is documented and to constantly improve this cycle by learning form what has been done.

In our context, to document what to do must be seen as the process of carefully examine the service levels really needed and the determination of which services will be outsourced and which services should be kept in house. For this process, a real integrated approach should be taken which consists of four areas, each dealing with respect to people, technology and processes. The four areas are:

- Strategy
- Objectives
- Critical Success Factors
- Performance Measurement

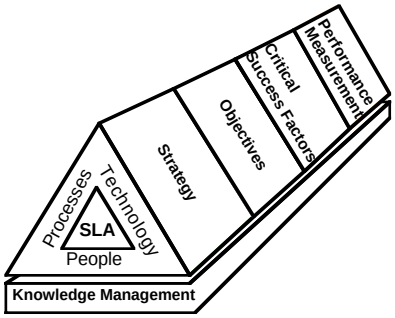


Figure 2 Integrated Approach

The integrated thinking in the "prism" depicted in Figure 2 leads to a greater intelligibility of business needs, the forces driving change, the current processes, and the vision of the business in the future. This can lead to opti-

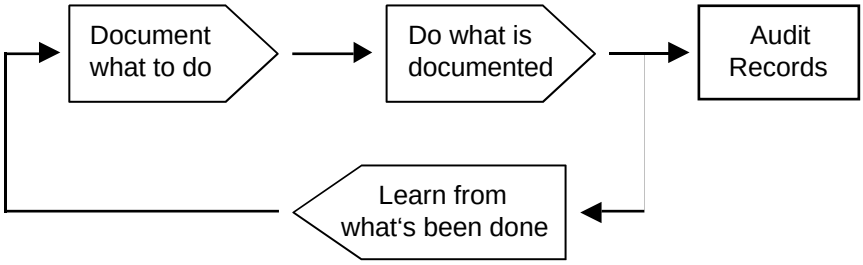


Figure 1 Management Environment

misations with parallel improvements in the business processes, technology, organisational design, and infrastructure as well as cultural changes.

Negotiating Service Levels

As we have seen in the previous section, there are a lot of factors, which have to be taken into account when service levels are defined. Principally service levels have to be negotiated between end-users and the service provider, e.g. outsourcing partner. When dealing with outsourcing IT-Systems or business processes which rely mainly on IT-Systems, there is often a strong need to support end-users in adapting business needs to IT systems and processes. It is, however, a good idea to hire an independent moderator for this task.

Figure 3 depicts the process of negotiating service levels. While looking at the service levels on one side – assuming that there is some common understanding of "high" and "low" service levels – the elapsed time during the process is drawn on the horizontal axis.

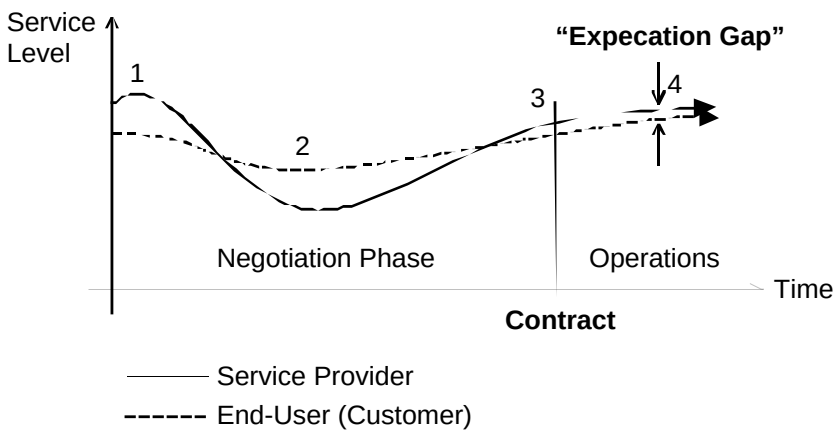


Figure 3 Negotiating Service Levels

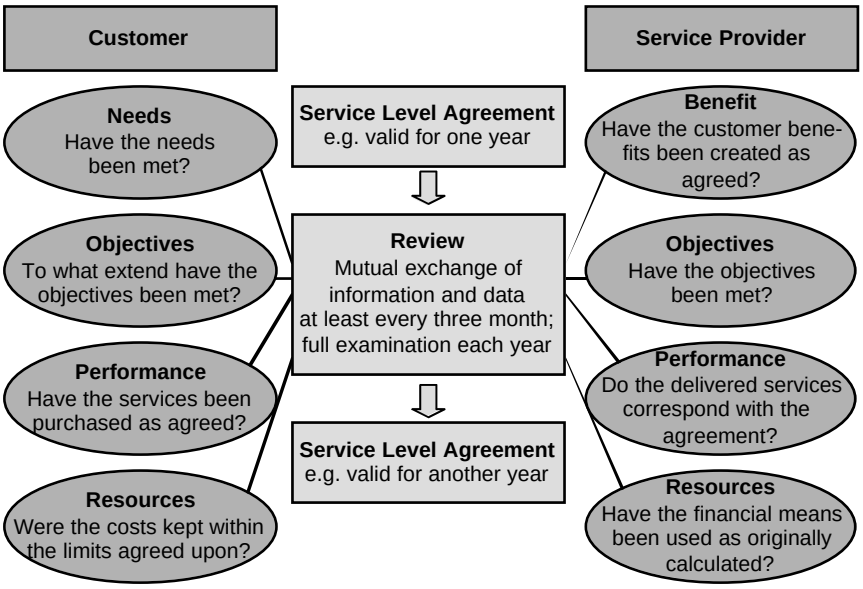


Figure 4 Continuously Managing Expectations

During the first steps of the negotiation phase, the service level needed and the service level offered from the service provider often do not match. Either the service level offered is much higher than what the customer request (1) or the customer expects much more than the service provider offers (2). The end of the negotiation phase should result in the point that the service level offered meets or slightly exceeds the service level demanded (3). After the Contract has been signed, which means that an agreement has been found, the service level should be constantly monitored and adapted, such that the "expectation gap" – the gap between the offered and expected service level – remains small (4). A process for constantly monitoring service levels is described in the following section.

Continuously Managing Expectations

As described above, during the lifetime of an outsourcing contract – i.e. Service Level Agreement – both, the service level offered as well as user's expectations have to be periodically reviewed. Figure 4 depicts the tasks to be carried out during a review process.

The permanent improvement of the process depicted in Figure 4 – a responsibility for management level, – should be institutionalised so that optimised structures can also adapt to future requirements. Such quality control measures ensure that the goal

of the company purchasing the service and the service provider are balanced and harmonised.

Risk Optimisation

Implementing Service Level Agreements effectively and efficiently solves typical problems like

- Inability to detect problems early
- Insufficient number of checkpoints
- Staffing problems

Service Level Agreements also feature result-oriented procedures, supported by appropriate techniques and tools. In this sense, Service Level Agreements support the idea of risk management in the following four areas:

- *Objectives*: Articulate and clarify business objectives
- *Risks*: The extent and magnitude of risks that might preclude or enhance the achievement of those objectives can be identified
- *Controls*: Appropriate controls are designed and implemented for reducing the risks identified. These controls must be properly aligned with the company's risk profile
- *Alignment*: Finally, it is imperative that objectives, risk and controls are aligned both horizontally (that is, not conflicting with the activities of other business units) and vertically (that is, consistent with the objectives of the overall entity)

Conclusion

Service Level Agreements strongly shape the relationship between customer and service providers and help create an atmosphere of co-operation on a partnership basis. Moreover, Service Level Agreements that are successfully anchored in the company culture lead to increased satisfaction, make internal and external benchmarking possible, and provide objective measurements as means to allocate and charge service. At the same time, they close the gap between what management expects would have been done and what really is going to be done. Regardless whether Service Level Agreements are introduced to buy services from an outsourcing provider or to transparently define services of an internal service department, it helps to set up clear rules and responsibilities and allows managing expectations of both sites, the customers and the service provider.

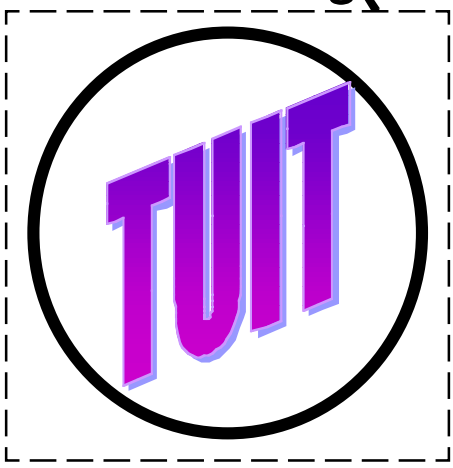
Dr. Christoph A. Burkhardt,
Leader "Telecom and Network Services",
PricewaterhouseCoopers, Zürich

References

- "Service Level Agreements gezielt einsetzen", Sylvia Enkelmann-Ackermann und Marion Bundi, IOmanagement, Nr.3/1999
- "Life Cycle Management for Dependability", Felix Redmill and Chris Dale (Eds), Springer; 1997

Cut out and save – to be used when required – a MUST for every computer auditor!

Guard it with your life. These TUITs have been hard to come by, especially the round ones. This is an indispensable item. It will help you become a much more efficient worker. For years, we have heard people say, "I'll do it as soon as I get a round TUIT". Now that you have a round TUIT of your very own, many things that have needed to be done, will finally get accomplished.



Checklist

Beurteilung Outsourcing-Verträge

Auf der ISACA-Homepage verfügbar!

Die IG Outsourcing des ISACA Switzerland Chapters erarbeitete in den letzten Jahren eine Checklist für die Erstellung und Revision von Outsourcing-Verträgen im Informatikbereich. Grundlage dazu legte vor allem Johann Krebs, der für seinen Arbeitgeber eine solche Checklist erarbeiten musste. Wir verdanken Johann und der UBS ausdrücklich, dass das Copy Right an dieser Checklist an die ISACA abgetreten wurde.

Die Struktur der Checklist geht davon aus, dass ein *Rahmenvertrag* vorhanden ist. Fehlt ein solcher, muss an der Stabilität des Outsourcing an sich gezweifelt werden. Im ersten Teil der Checklist werden demnach allgemein Grundsätze und Vertragsbestimmungen behandelt. Sodann tritt die Checklist auf Aspekte der *Leistungsbeschreibung*, der *Sicherheit* und schliesslich der *Revision* ein. Die Checklist nimmt an, dass das Vertragswerk grundsätzlich offen gestaltet ist und sich auf Anhänge, die fallweise zu erstellen und bearbeiten sind, stützt. Es ist zudem offensichtlich, dass die Checklist weitgehend generische Elemente enthält; sie muss also zurecht geschnitten werden.

Diverse Mitglieder der IG testeten die Checklist bei ihren Unternehmungen und konnten wesentlich zur Verbesserung der ursprünglichen Version beitragen. Die IG diskutierte die Aspekte in mehreren Sitzungen eingehend und ist heute daran, Kriterien für die Messbarkeit von Grössen in den Service Level Agreements zusammenzutragen. Die IG hat sowohl Mitglieder, die für Outsourcing-Nachfrager oder deren Revisoren tätig sind, als auch solche, die für Outsourcing-Anbieter oder deren Revisoren arbeiten. Dementsprechend beleuchtet die Checklist *beide* Gesichtspunkte. Im Gegensatz dazu beschränkt sich die letztes Jahr publizierte internationale Guideline der ISACA betreffend Outsourcing lediglich auf den Gesichtswinkel des Outsourcing-Nachfragers.

Die IG ist überzeugt, für den Berufsstand ein brauchbares Instrument geschaffen zu haben und nimmt Anregungen zur Verbesserung laufend entgegen.

Die Checklist ist auf der homepage http:/www.isaca.ch/ abrufbar. Die IG ermutigt die Mitglieder, die Checklist zu gebrauchen. ISACA erwartet, dass beim Kopieren und Verwenden der Checklist ein Hinweis auf das Copy Right (© ISACA Switzerland Chapter) angebracht wird.

Die IG (mitgearbeitet haben bisher: Jean Bloch, Max Bretscher, Pierre Ecoeur, Ueli Engler, Matthias Habegger, Johann Krebs, Walter Muster, Stefan Tanner, Robert Thommen und Peter Zürrer)

Résumé français: La “Checkliste examen d’un contrat d’externalisation”

disponible sur les pages Web de l’ISACA-Suisse (www.isaca.ch)

Ce précieux et très complet instrument peut être téléchargé mais il n’existe malheureusement qu’en allemand et anglais à l’heure actuelle. Si quelqu’un veut participer à sa traduction en français (ou sponsoriser une telle traduction), prendre contact avec M. Huissoud (031/323 10 35).

Outsourcing von Informatikleistungen[1,2]

Ausgangslage: Monopol und Vertrauen

Nehmen wir einmal an, es gebe im Flugverkehr ein Monopol. Sie müssten für Reisen – zum Beispiel von Zürich nach Bern – das Flugzeug nehmen und zwar das der Monopolgesellschaft A-Air. Diese Gesellschaft besitzt erstklassiges Flugmaterial, top ausgebildetes Personal, einen exzellenten Kundenservice, einen anerkannt guten Unterhalt. Sie belegt in internationalen Rankings bezüglich der Sicherheit immer einen der ersten Plätze. Sie untersteht einer strengen Aufsicht, ja die Verletzung ihrer Servicepflicht wird sogar strafrechtlich geahndet.

Sie – qualitätsbewusst, wie Sie sind – fliegen seit Jahren gut mit A-Air, haben Vertrauen in sie und lehnen sich im weichen Flugzeugsessel mit einem guten Gefühl zurück. Nun aber muss diese Gesellschaft sparen. Sie hat sich vielleicht etwas übernommen, sich statt nur Nötiges auch Luxus geleistet.

Outsourcing verspricht Kostenoptimierung: Und das Vertrauen?

Die Monopolgesellschaft verspricht sich Kostensenkungen durch Outsourcing. Sie behält das Monopol, aber sie lagert den gesamten Flugbetrieb aus auf die B-Air.

Würden Sie sich – qualitätsbewusst, wie Sie immer noch sind – mit einem ebenso guten Gefühl in dieses Flugzeug setzen, das offensichtlich in einem sehr schlechten Zustand ist? Mit einem Piloten, dem Sie nicht zutrauen, das Flugzeug von der Piste weg, geschweige denn auch heil wieder hinunter zu bringen? Mit einem himmeltraurigen Service? Sicher nicht! Hier – so würden Sie zu Recht geltend machen – wird am falschen Ort gespart. Sie hätten kein Vertrauen in die B-Air.

Würden Sie sich aber mit einem guten Gefühl in das Flugzeug der C-Air setzen? Sie sehen keinen Unterschied? Flugzeug, Personal und Service machen denselben guten Eindruck wie bei der A-Air. Aber genügt das, Ihr Vertrauen zu gewinnen?

Für eine gültige Beurteilung müssten Sie wohl mehr wissen, etwa:

- dass die C-Air anderen Regeln untersteht, dass sie weniger streng eingebunden ist,
- dass die zuständige Aufsichtsbehörde weniger Kontrollbefugnisse, weniger griffige Kontrollinstrumente besitzt,
- dass die Verletzung der Servicepflicht durch die C-Air nicht strafrechtlich geahndet wird, oder
- dass Sie als Passagier(in) einen aufwändigeren Weg einzuschlagen haben, um im Schadenfall zu Ihrem Recht zu kommen.

Nun? Wie steht es jetzt?

IT beim Monopolisten Staat

Sie haben es sicher schon lange erraten: Der Monopolist ist der Staat, zu dem Sie für bestimmte Zwecke hin müssen, ob Sie es wollen oder nicht: Sie können nicht argumentieren, Sie könnten Ihr Geld sinnvoller anderen Institutionen zuwenden statt dem Steueramt; Sie können der Untersuchungsrichterin nicht entgegen-

halten, Sie würden sich lieber ein Zimmer in einem Hotel auf einer Südseeinsel nehmen statt im Untersuchungsgefängnis; und es nützt Ihnen auch nichts, wenn Sie lieber Ihrer Architektin mehr bezahlen statt dem Bauamt für die Baubewilligung.

Wenn der Staat wie in der Vergangenheit – mehr oder weniger allein, mehr oder weniger zentral und mehr oder weniger effizient – seine Informatik selber besorgt, betreibt und betreut, dann macht er dasselbe wie die A-Air im Ausgangsbeispiel. Und wenn er Kosten senken muss oder nötige Weiterentwicklungsschritte nicht mehr aus eigener Kraft bewältigen kann, dann kommt – auch bei ihm – rasch Outsourcing als "Erfolgsrezept" daher.

Qualitätssicherung bei Outsourcing: Instrumente und Voraussetzungen

Während sich in den dazu geführten Diskussionen die einen von Outsourcing alles Erdenkliche erhoffen, weckt für andere Outsourcing schlimmste Befürchtungen: Diese Diskussionsebene illustriert das Beispiel der B-Air. Wenn Sie die jüngsten Diskussionen nach dem schweren Eisenbahnunglück von Anfang Oktober 1999 in Grossbritannien verfolgt haben, wo Kostenoptimierung der privaten Betreibergesellschaft zu unerträglichen Sicherheitsdefiziten geführt haben soll, oder sich an den letztjährigen Zusammenbruch der privatisierten neuseeländischen Stromversorgung wegen des nicht genügend unterhaltenen Versorgungsnetzes erinnern, dann können Sie Bedenken, dass der Kostensenkungsdruck auch zu unerwünschten Effekten führen kann, nicht von der Hand weisen. Allerdings gibt es Instrumente zur Eingrenzung dieser Risiken:

- Eine klare und detaillierte *quantitative und* vor allem auch *qualitative Definition der Leistungen*,
- eine unanfechtbare *Leistungskontrolle*,
- wirksame *Massnahmen* für den Fall, dass vereinbarte und erbrachte Leistung auseinanderklaffen,

das sind unverzichtbare Voraussetzungen für den Erfolg eines Outsourcing-Projektes. Hoffnung in die Qualität der Outsourcingnehmerin und ihres Personals ist nett, Vertrauen ist gut, Kontrolle aber – auch hier – besser.

Allerdings: Damit diese Qualitätssicherung auch erfolgreich sein kann, braucht es auf der Seite der outsourcenden Verwaltung unabdingbar professionelles Know-how *in-house*, also genügend hochqualifiziertes Personal. Es ist bekannt, dass die grössten Outsourcer aus der Privatwirtschaft heute wieder daran sind, das kurzsichtig abgebaute innerbetriebliche Know-how mühsam und teuer wieder aufzubauen! Wer die oftmals schon blauäugig anmutenden Beurteilungen des Spareffektes bei Outsourcing-Projekten ansieht, wird den Eindruck nicht los, dass dieser Aspekt – aber nicht nur bei staatlichen Vorhaben – häufig viel zu wenig beachtet wird. Zu einer sorgfältigen Vorbereitung von Outsourcing-Projekten würde aber gerade eine umfassende und ehrliche Beurteilung auch in dieser Hinsicht gehören – denn wozu soll Outsourcing noch gut sein, wenn wir die gleiche Leistung schliesslich nicht günstiger erhalten?

Die datenschutzrechtliche Seite von Outsourcing

Die eben dargestellte Seite der Diskussion ist aber nicht nur und nicht primär datenschutzrechtlicher Natur. Vielmehr treffen wir den Kern der datenschutzrechtlichen Diskussion mit dem Beispiel der C-Air. Es geht aus Datenschutzsicht nicht um bessere oder schlechtere Computer, nicht um schnellere oder langsamere Drucker, nicht um Datentransferraten, Antwortzeiten oder Systemverfügbarkeit, sondern um die *Grundrechte der betroffenen Personen*:

- um den Schutz vor unzulässiger Bearbeitung ihrer Daten,
- um Gesetzmässigkeit und Verhältnismässigkeit beim Bearbeiten,
- um den Schutz vor unbefugtem Zugriff,
- um das Recht der betroffenen Personen auf Auskunft, Einsicht und Berichtigung und
- um die Aufsicht über die Datenbearbeitung.

Auf diese Seite der Problematik wollen wir etwas genauer eingehen.

Im Wes(t)en nichts Neues

Nun macht ja die staatliche Verwaltung seit "alters" her – wenn man bei IT von Alter sprechen kann – nicht alles selber, sondern zieht externe Unternehmen bei. Ihrem Wesen nach ist Outsourcing also nichts Neues: So hat die Verwaltung auf dem Markt nicht erhältliche Spezialsoftware nur selten noch selber entwickelt, sondern zunehmend durch externe Unternehmen entwickeln lassen. Auch die Wartung von Hard- und Software und die Planung und Steuerung von (grösse-

ren) IT-Projekten hat sie seit langem zunehmend ausgelagert. Solches Outsourcing[3] galt – als Teil der Bedarfsverwaltung – auch ohne gesetzliche Grundlage als zulässiges privatwirtschaftliches Handeln des Staates[4].

Herkömmliche datenschutzrechtliche Einfassung

Den datenschutzrechtlichen Anliegen konnte Rechnung getragen werden, indem wenn immer möglich auf den Zugriff auf Echtdaten verzichtet wurde. Für den Fall, dass der Zugriff auf Personendaten nicht ausgeschlossen werden konnte, behalf man sich mit den datenschutzgesetzlichen Vorkehren für die *Auftragsdatenbearbeitung* – obwohl ja ein materielles Bearbeiten gerade nicht bezweckt wurde, sondern nur ein Zugriff nicht ausgeschlossen werden konnte. Die Verantwortung – so sehen die Datenschutzgesetze für die Auftragsbearbeitung vor – bleibt bei der auftraggebenden Behörde[5], und der Datenschutz ist "durch Auflagen, Vereinbarung, Festsetzung einer Konventionalstrafe oder auf andere Weise"[6] sicherzustellen.

Das mag in vielen Fällen genügen, auch wenn häufig bestimmte Fragen offen bleiben. So bleibt häufig unklar, welches Datenschutzrecht anwendbar ist: Die bundesdatenschutzgesetzlichen Bestimmungen für Datenbearbeitung durch Private, weil das Unternehmen dem Privatrecht untersteht, oder die entsprechenden öffentlichrechtlichen Bestimmungen, weil es um das Datenbearbeiten durch Behörden geht? Fraglich bleiben damit auch die Zuständigkeit und Befugnisse der Datenschutzaufsicht. Und schliesslich ist auf bloss vertraglichem Wege auch keine Ausdehnung des Geltungsbereiches personal- oder beamtengesetzlicher Amtsgeheimnisbestimmungen (und vor allem der entsprechenden Strafbestimmungen im Strafgesetzbuch) zu bewerkstelligen.

Herausforderung durch neue Entwicklungen

In jüngerer Vergangenheit wird nun aber eine Entwicklung sichtbar, welche die Frage aufwirft, ob der Schutz der Grundrechte auf dieser behelfsmässigen Grundlage noch ausreichend gewährleistet werden kann.

Wir müssen uns ernsthaft fragen, ob nicht irgendwo zwischen der bisher gängigen Auslagerung von einzelnen Dienstleistungen – sozusagen vom externen Putzenlassen von Druckern – und dem Outsourcing ganzer IT-Umgebungen[7] eine qualitative Grenze überschritten wird – insbesondere wenn wir unter IT nicht bloss den PC am Arbeitsplatz verstehen, auf dem mit Standardanwendungen Verfügungen geschrieben werden, sondern mit einem etwas neuzeitlicheren Verständnis von IT auch in Betracht ziehen, welches Entwicklungspotenzial bei der Automatisierung von (Verwaltungs-)Abläufen in vernetzten Systemen absehbar ist.
Das Stichwort *eGovernment* – wenn man darunter mehr versteht als die blosse Wiedergabe von Schalteröffnungszeiten der Verwaltung im Internet oder die Möglichkeit, Formulare herunterzuladen! – lässt in Ansätzen die künftigen Entwicklungsmöglichkeiten ahnen. Am 4. Symposium für Datenschutz und Informationssicherheit hat Prof. Ueli Maurer den Weg zur Ermöglichung von elektronischen Volksabstimmungen aufgezeichnet. Es sind aber bereits in näherer Zukunft weitere Anwendungen denkbar, bei welchen die Informatik mehr als die heutige Unterstützungsfunktion übernimmt, z.B. bei der automatisierten Abwicklung von Verfahren. Ich denke etwa an in der Praxis fast schon voraussetzungslos gewährte Verlängerungen von Einreichungsfristen, von bestimmten Verlängerungsbewilligungen usw. Man füllt übers Internet ein Formular aus und der Computer auf der Verwaltungsseite erlässt sogleich die entsprechende Verfügung. Denkbar ist aber auch die Abwicklung von Verfahren, bei welchen die Überprüfung der Voraussetzungen automatisiert erfolgen kann: So könnte eine Gesuchstellerin etwa ihr Gesuch um Krankenkassenprämienverbilligung auf elektronischem Weg stellen. Die amtliche Abwicklung könnte durchaus auch automatisiert erfolgen, wenn auf elektronischem Weg die Voraussetzungen durch Datenbankabfragen bei der Einwohnerkontrolle, der Steuerverwaltung und einer Krankenkassenprämiendatenbank abgeklärt werden können. Weil für die Zusprechung der Prämienverbilligung kein Ermessensspielraum besteht, kann dann auch die Verfügung automatisiert elektronisch erlassen werden.

Verwaltungsrechtlicher Exkurs: Tauglichkeit der überkommenden Kategorie der Bedarfsverwaltung?

Der Blick auf solche Entwicklungsmöglichkeiten lässt die Frage dringend erscheinen, ob das Outsourcing, mindestens wenn ganze IT-Umgebungen aus der Verwaltung ausgelagert wer-

den, wegen des zunehmenden Eingriffspotenzials einer modern verstandenen IT und der potenziellen Verschlechterung der Position der betroffenen Personen nicht einer *besseren rechtlichen Einbindung* bedarf.

Aus verwaltungsrechtlicher Sicht heisst das: Taugen die hergebrachten Unterscheidungen zwischen Eingriffs-, Leistungs- und Bedarfsverwaltung noch? Ist modern verstandene Informationstechnologie wirklich einfach "administrative Hilfstätigkeit"? Und ist der daraus gezogene Schluss, dass nämlich diese Tätigkeit des Staates – und ebenso die Auslagerung solcher Tätigkeiten – keiner rechtlichen Grundlage bedarf, noch sachgerecht? Wenn man an den hergebrachten Unterscheidungen grundsätzlich festhalten will, müsste wohl ernsthaft geprüft werden, ob nicht eine Art "Zwischenschicht" im Sinne einer *qualifizierten Bedarfsverwaltung* [8] eingezogen werden müsste. Als qualitative Kriterien kämen etwa die Sensitivität der Aufgabe[9], das Risikopotenzial der Tätigkeit, die Bedeutung der Aufgabe für die (staatliche) Aufgabenerfüllung, die (relative) Austauschbarkeit der Leistungserbringer oder die Nähe zu einer hoheitlichen Tätigkeit[10] in Frage. Es wäre in der Folge zu prüfen, ob bei der qualifizierten Bedarfsverwaltung wirklich generell vom Erfordernis einer gesetzlichen Grundlage für die Auslagerung abgesehen werden kann[11].

Bessere rechtliche Einbindung: Inhalt und Massstab

Aus Datenschutzsicht – es gibt aber auch andere Gründe für eine solche Einbindung[12] – bedürfen folgende Punkte einer Regelung[13]:

- Das für das Datenbearbeiten durch *Behörden geltende Datenschutzrecht* – inklusive der Informatiksicherheitsregelungen – muss auch für das Bearbeiten auf outgesourcter Infrastruktur gelten.
- Die *Verantwortung* für das Datenbearbeiten muss ganz klar *bei der mit der Aufgabe betrauten Behörden* bleiben: Sie darf sich durch das Outsourcing von Informatik-Dienstleistungen nicht aus der Verantwortung stehlen können.
- Daten dürfen *erst* über outgesourcte Infrastruktur bearbeitet werden, wenn sichergestellt ist, dass sie – ihrer Sensitivität entsprechend – durch technische und organisatorische Massnahmen *wirksam vor unbefugter Einsichtnahme geschützt* sind.
- Das für die Aufsicht über das behördliche Datenbearbeiten zuständige Datenschutzaufsichtsorgan hat die *Aufsicht* auch über das Datenbearbeiten auf outgesourcter Infrastruktur auszuüben – *mit denselben Befugnissen und mit denselben Instrumenten*, also beispielsweise auch mit dem Recht, anlassfrei und unangekündigt Kontrollen durchzuführen – nicht nur im Interesse der betroffenen Personen, sondern auch im Interesse der verantwortlichen Behörde.
- Die mit der Leistungserbringung durch das externe Unternehmen betrauten Mitarbeiter(innen) sind den für die behördliche Datenbearbeitung geltenden *Geheimhaltungsbestimmungen* samt den entsprechenden strafrechtlichen Sanktionierungsmöglichkeiten zu unterstellen. Dazu bedarf es wohl eines Gesetzes.

Nur mit diesen Regelungen kann vermieden werden, dass nicht die Bürger (innen) als Objekte staatlicher Datenbearbeitung die Outsourcing-Rechnung bezahlen müssen!

Die durch diese Rahmenbedingungen entstehenden Kosten sind nicht etwa "Zusatzkosten", welche die Aufgabenerfüllung erschweren. Der *Schutz der Grundrechte* der Personen, über die Behörden Daten bearbeiten, ist in einem freiheitlichen Rechtsstaat *Teil der Aufgabenerfüllung* und ein *urliberales Postulat*.

Es gereicht dem Kanton Zürich zur Ehre, dass er – soweit ersichtlich als erstes Gemeinwesen in der Schweiz – den Regelungsbedarf erkannt hat und am 23. August 1999 ein Gesetz über die Auslagerung von Informatikdienstleistungen beschlossen hat[14] (die Referendumsfrist ist bekanntlich anfangs November 1999 ungenutzt verstrichen). Ob die Bestimmungen des Gesetzes in der konkreten Umsetzung allerdings die eben genannten Forderungen zu erfüllen vermögen, wird erst die Zukunft weisen.

Beat Rudin, Datenschutzbeauftragter des Kantons Basel-Landschaft[15]

Endnoten

1 Überarbeitete Version eines am 28. Oktober 1999 am Symposium für Datenschutz und Informationssicherheit an der ETH Zürich gehaltenen Referates. Der Vortragsstil wurde beibehalten.

2 Mit freundlicher Genehmigung des Autors erfolgt der Nachdruck aus FAKTEN 4/99.

3 Die Breite der möglichen IT-Outsourcing-Gegenstände mag illustriert werden durch die folgende Übersicht (nach Alfred Büllesbach, Outsourcing in

der öffentlichen Verwaltung, in: Wilfried Köhler-Frost (Hrsg.), Outsourcing – Eine strategische Allianz besonderen Typs, 2. Aufl., Berlin 1995, 116. ff.): Planung von IT-Leistungen; Ressourcen-Beschaffung (Hard- und Software, Personal und Know-how); Rechenzentrumsdienstleistungen (wie Betriebssystempflege, Operating, Betrieb von Datenbanksystemen/Tools und/oder von Anwendungssoftware, Betrieb von Batch-Anwendungen: Betrieb von Online-Anwendungssystemen, Datensicherung, Systemdokumentation bis hin zur Übernahme eines ganzen Rechenzentrums); Bereitstellung und Betrieb von Local, Wide oder Global Area Networks (wie Netzwerkbereitstellung, Netzwerkbetrieb und –management, Bereitstellen von Trägernetzen oder Übernahme eines vorhandenen Netzes, Recovery-Services, Facilities- und System-Management, Client/Server-Services, Wartung, Informationsverarbeitungs-Controlling, Haustechnik, Datenvernichtung

4 Vgl. dazu etwa Ulrich Häfelin/Georg Müller, Grundriss des Allgemeinen Verwaltungsrechts, 3. Auflage, Zürich 1998, Rz. 225; René Rhinow/Beat Krähenmann, Schweizerische Verwaltungsrechtsprechung, Ergänzungsband, Basel/ Frankfurt a.M. 1990, Nr. 47 B.I.a, Nr. 59 B.II.b; Rolf H. Weber, Outsourcing von Informatik-Dienstleistungen in der Verwaltung, in: ZBl (Schweizerisches Zentralblatt für Staat- und Verwaltungsrecht) 1999, 97 ff., insb. 100 ff.

5 So etwa § 4 des basellandschaftlichen Gesetzes vom 7. März 1991 über den Schutz von Personendaten (Datenschutzgesetz/ DSG-BL, SGS 162, im Internet abrufbar über http://www.bl.ch/docs/recht/sgs_1-2/162.0.htm): "Für den Datenschutz ist diejenige Behörde verantwortlich, die in Erfüllung ihrer gesetzlichen Aufgaben Personendaten bearbeitet oder *bearbeiten lässt*."

6 So wörtlich § 13 DSB-BL.

7 Z.B. durch die Auslagerung der Informatikämter der Kantone St. Gallen und Zürich und den Zusammenschluss zur Abraxas Informatik AG.

8 Wohl nicht ganz dasselbe meint Weber (En. 4) mit der "(gegebenenfalls qualifizierten) Bedarfsverwaltung" (108 mit Verweis auf 102 f.). Insbesondere fehlen Hinweise auf Kriterien für die Qualifikation und zieht der Autor keine spezifischen Schlussfolgerungen aus einer Qualifikation.

9 Die Bearbeitung von Strassenunterhaltsdaten qualifiziert eine Aufgabe weniger als die Bearbeitung von Gesundheitsdaten oder Verdachtsdaten der Polizei.

10 In der Lehre werden bestimmte Datenbearbeitungen wegen ihres nahen Bezugs zu hoheitlichen Tätigkeiten als Teil der hoheitlichen Tätigkeit betrachtet, etwa bei Polizei- oder Sicherheitsbehörden, Steuer- und Finanzverwaltung, mit der Folge, dass selbst statistische Bearbeitungen als hoheitliche Tätigkeit gelten (so Büllesbach) (En. 3), 120 ff.).

11 Ohnehin schaut die herkömmliche Betrachtungsweise gleichsam in die falsche Richtung: Der Staat darf, so die herkömmliche Lehre, bei der (einfachen) Bedarfsverwaltung auch ohne gesetzliche Grundlage tätig werden. Beim Outsourcing geht es hingegen gerade umgekehrt um das Nicht-(mehr-selber-)Tätigwerden. Können die Schlussfolgerungen der einen Blickrichtung unbesehen auf die andere Blickrichtung übertragen werden?

12 So beurteilt etwa nach Medienberichten das Bundesamt für Polizei "die Privatisierung von Informatikdienstleistungen für Polizeisysteme aus rechtlichen Gründen, aus Gründen der Daten- und Informatiksicherheit sowie aus polizeilichen Geheimhaltungs- und Sicherheitsinteressen als problematisch" erachte (NZZ, 14.01.2000, S. 41).

13 Vgl. auch Weber (En. 4), 120 ff. mit weiteren Hinweisen.

14 Amtsblatt des Kantons Zürich Nr. 35, 3. September 1999 (abrufbar über http://www.amtsblatt.zh.ch (Rubrik Archiv).

15 Dr. iur. Beat Rudin, Datenschutzbeauftragter des Kantons Basel-Landschaft, Justiz-, Polizei- und Militärdirektion,
Postfach, 4410 Liestal,
datenschutz@jpm.bl.ch,
http://www.baselland.ch/datenschutz.htm

Résumé: Outsourcing des prestations informatiques

L'auteur montre les risques liés à l'externalisation par une collectivité publique de ses prestations informatiques. Les mesures pour limiter ces risques existent: une définition claire des prestations, un contrôle efficace des prestations apportées et des mesures efficaces pour corriger tout écart constaté. Elles impliquent cependant que l'entreprise qui externalise a conservé le know-how nécessaire à l'exercice de ces tâches de contrôle!

Si l'externalisation des tâches de conception informatique est une chose aujourd'hui courante et qui n'exige en principe pas de base légale particulière, l'externalisation de l'exploitation pose en revanche d'importants problèmes de protection des données. La tendance qui se dessine sous la formule e-Government est à cet égard symptomatique: votations par Internet, actes de procédure civile ou pénale par e-mails, requête électronique pour obtenir une subvention, etc.

L'auteur plaide pour un renforcement de l'exigence d'une base légale dans ces cas, afin de régler notamment le droit de la protection des données applicable (dispositions pour les administrations publiques ou les entreprises privées?), le principe de l'inaliénabilité de la responsabilité du maître des fichiers, la preuve à apporter de l'efficacité des mesures destinées à assurer la confidentialité des données, etc. L'exemple de la loi zurichoise en matière d'externalisation de prestations de services (http://www.amtsblatt.zh.ch) est certainement une piste à suivre.

Kommentar zum EBK-RS 99/2

Outsourcing aus Sicht eines Informatik-Revisors

Mitglieder der IG Outsourcing der ISACA (Switzerland Chapter) haben sich bereits im Vorfeld des Vernehmlassungsverfahrens mit dem "Rundschreiben der Eidgenössischen Bankenkommission zum Thema Outsourcing" (RS)[1] auseinandergesetzt. So hatte die Treuhand-Kammer anlässlich der Tagung "Aktuelle Themen der Revision von Banken und Effektenhändlern" vom 18. November 1998 in Zürich den damaligen Entwurf des Rundschreibens kritisch unter die Lupe genommen. Die EBK bereinigte in der Folge diverse kontroverse Punkte. Die endgültige Fassung enthält nun einige Elemente, die für die Revision von gewisser Tragweite sind. Die folgenden Bemerkungen treten jedoch nicht auf die grundsätzlichen Fragen ein, obschon hier brisanter Zündstoff für ausgiebige Diskussionen liegen könnte, sondern konzentriert sich auf Kernfragen der Informatik-Revision in diesem Zusammenhang.

Obschon CobiT[2] die Frage des Outsourcing nicht explizit anspricht, sind die Zusammenhänge auf allen Ebenen (Planung & Organisation, Beschaffung & Unterhalt, Auslieferung & Unterstützung sowie Überwachung) sofort ersichtlich. Daneben ist die vom Standards Board ISACA 1999 verabschiedete Guideline[3] bezüglich Outsourcing direkt auf das RS anzuwenden. Die von der IG Outsourcing des ISACA (Switzerland Chapter) 1996–1999 geschaffene Outsourcing-Vertrags-Checklist[4] ist als Hilfsmittel zur Prüfung der einschlägigen Belange zusätzlich zu empfehlen.

Zum RS werden mit Sicherheit sehr umfangreiche Diskussionen und Kommentare erfolgen. Diese Betrachtungen nehmen denn auch nicht für sich in Anspruch, allumfassend zu sein. Aus Sicht der Informatik-Revisors seien dennoch die wichtigsten Aspekte kurz beleuchtet.

Definitionen

Das RS definiert Outsourcing als wesentliche Tätigkeit eines Unternehmens, die dauernd unter der Verantwortung eines Dritten erbracht wird. Stichworte sind dabei die Ausdrücke "wesentlich" und "dauernd". Verschiedene Firmen, so auch Banken, haben sich in den letzten Jahren entschlossen, sich auf ihr sogenanntes "Kerngeschäft" zu konzentrieren und die restlichen Tätigkeiten ausser Haus zu vergeben. Der Umkehrschluss liegt also nahe, dass ausser Haus vergebene Tätigkeiten demnach nicht "wesentlich" sein können! Ganz abgesehen davon, dass sich jedes ISACA-Mitglied im Falle von Outsourcing dieser Dienstleistung gegen eine derartige Klassierung der Informatik vehement zur Wehr setzen würde, nennt das RS "Informatik" jedoch explizit als prominentes Beispiel. Ob darunter jeweils die gesamte Palette bzw. jeglicher Teil der Dienstleistung zu verstehen ist, kann Anlass zu Diskussionen geben. So könnte m.E. der ausser Haus vergebene *Bancomat* sehr wohl in die Definition fallen, unter andern Umständen (wahrscheinlich Nebensächlichkeit z.B. für Privatbanken) die Voraussetzung der Wesentlichkeit nicht erfüllen.

In der Folge muss die (Informatik-) Revision abwägen, ob das RS für den vorliegenden Fall überhaupt zutrifft. Im Zweifelsfalle bin ich der Meinung, dass die Gültigkeit vorhanden ist. Die Informatik besitzt heute im Aspekt "Abhängigkeit" eine Bedeutung, die nur in wenigen Fällen als "unwesentlich" eingestuft werden darf.

Geltungsbereich und Zulässigkeit

Das RS gilt für alle Banken und Effektenhändler in der Schweiz, inklusive Niederlassungen ausländischer Institutionen. Unter diesem Titel sind auch Einschränkungen und Ausnahmen erwähnt. Sie werden nachstehend bei den jeweiligen Grundsätzen gestreift.

Voraussetzungen – die Grundsätze

Grundsatz 1: Bestimmung des auszulagernden Geschäftsbereiches

Dieser Absatz hält u.a. fest: "Für den auszulagernden Geschäftsbereich sind die genauen Anforderungen für die Leistungserbringung festzulegen und zu dokumentieren."

Diese Forderung ist für die Informatik-Revision von etwelcher Bedeutung, weil damit die Systemgrenzen angesprochen sind. Es ist zwar unbestritten (Grundsatz 3), dass die Verantwortung immer im Schosse der Unternehmung liegt, doch werden durch das Outsourcing normalerweise Zuständigkeiten auf der operationellen Ebene aufgeteilt. Für die Informatik-Revision ist es also wichtig zu wissen, welche Bereiche aufgrund welcher Vereinbarungen bzw. Zielvorgaben durch wen wie und wann zu bearbeiten sind. Nur aufgrund dieser Grundlage wird ein Soll-/Istvergleich erst möglich. Ein eingehendes Studium der Naht- bzw. Schnittstellenbeschreibungen muss demnach erfolgen, bevor die eigentliche Revisionstätigkeit aufgenommen wird.

Grundsatz 2: Auswahl, Instruktion und Kontrolle des Dienstleisters

In diesem Zusammenhang sind für die Informatik-Revision folgende Forderungen von wesentlicher Bedeutung:

- "Der ausgelagerte Geschäftsbereich ist in das interne Kontrollsystem der Unternehmung zu integrieren."
- " Die Unternehmung hat sich die … nötigen Einsichts-, Weisungs- und Kontrollrechte vom Dienstleister vertraglich einräumen zu lassen."

Auf den ersten Blick scheint ein Widerspruch zu den Bemerkungen zum vorstehenden Grundsatz 1 vorzuliegen: Einerseits Abgrenzung, andererseits Integration. Gerade diese technisch nicht immer leicht zu bewältigende Gratwanderung verlangt vom Beauftragten (und damit dessen Revision) grösste Aufmerksamkeit. Die Erfahrung im Bereich Outsourcing hat in der Vergangenheit verschiedentlich gezeigt, dass in Delikts- oder Konfliktfällen unzulängliche Vertragsteile zu unangenehmen Kosten- und Abhängigkeitsfolgen führten. Der Informatik-Revisor kann mit einer sorgfältigen Bearbeitung der erwähnten Vertragschecklist wertvolle Beiträge liefern.

Grundsatz 3: Verantwortung

Die Verantwortung bleibt bei der auslagernden Unternehmung. Der nachstehend erwähnte Grundsatz 7 bezüglich Revision und Aufsicht bringt es häufig mit sich, dass die Revision beim Dienstleistungserbringer einer einzigen Stelle anvertraut wird. Die entsprechende Berichterstattung wird allen Benutzern zur Verfügung gestellt. In einzelnen Fällen wird es nicht trivial sein, die Aussagen in einem Bericht dergestalt zu interpretieren, dass daraus eine Aussage bezüglich Ordnungsmässigkeit[5] bei der die Verantwortung tragenden Unternehmung abzuleiten. Die aktive und intelligente Beteiligung der Informatik-Revision ist einmal mehr gefragt.

Grundsatz 4: Sicherheit

Es handelt sich hier quasi um ein "Heimspielfeld" der Informatik-Revision. Die detaillierten Bestimmungen in diesem Grundsatz des RS weisen eindeutig in die Richtung der elektronischen Datenverarbeitung. Insbesondere die CobiT Kriterien Vertraulichkeit, Integrität, Gesetzeskonformität und Zuverlässigkeit sind direkt angesprochen.

Grundsatz 5: Geschäfts- und Bankgeheimnis

Die Bestimmung, dass die Vertraulichkeit der Datenbehandlung nicht nur gegen aussen (vom Dienstleistungserbringer aus gesehen), sondern auch zwischen den einzelnen Benützern gewährleistet sein muss, wird in der Praxis auf etwelche Schwierigkeiten stossen. Der Informatik-Revisor wird in die Tiefen der Betriebssysteme steigen müssen, um die Umsetzung und auch Durchsetzung der gewünschten Funktionentrennung zu eruieren und zu verifizieren.

Grundsatz 6: Kundenorientierung

Eine heikle Frage, die sich mir stellt, ist die Art der Datenübermittlung, weil das RS sowohl die uncodierte als auch codierte (gemeint ist wohl chiffrierte) Form der Übermittlung ins Ausland der Orientierungspflicht unterwirft. Eine enge Interpretation führt nach sich, dass z.B. jede Art von Internet-Banking, aber u.U. auch andere Übermittlungsverfahren via Satellit unter diese Bestimmung fallen! Abgesehen von der Frage, ob sich die Bankinstitute ihrer Pflichten bewusst sind, können in den Einzelfällen nur Spezialisten (und dazu zähle ich z.B. CISAs) gültige Antworten erarbeiten.

Grundsatz 7: Revision und Aufsicht

Bereits bei Grundsatz 3 (Verantwortung) vorstehend wies ich auf die wohl häufig anzutreffende Situation der Revision durch einen Dritten hin. Damit sind u.a. GzA4[6] und/oder SAS 70[7]

angesprochen. Beide Standardwerke weisen darauf hin, dass eine “eigene” Prüfung dann unabdingbar wird, wenn aus den Unterlagen keine zuverlässigen Schlüsse gezogen werden können. Im stark technisierten Umfeld der Auslagerung von Informatik kann wohl nur ein Spezialist gültige Antworten in dieser Hinsicht liefern bzw. in Zusammenarbeit mit dem Arbeitskollegen des Prüfers der Dienstleistungsgesellschaft extrahieren.

Grundsatz 8: Auslagerung ins Ausland

Diese Problematik wurde bereits beim Grundsatz 6 (Kundenorientierung) angetippt. Sie verschärft sich in jenen Fällen, wo eine permanente Auslagerung der Informationen im Ausland (d.h. der Dienstleistungserbringer befindet sich im Ausland) erfolgt. Vielfach ist es gerade bei internationalen Finanzunternehmungen anzutreffen, dass sich Dienstleistungszentren oder deren Ausweichsinstallationen im Ausland befinden. Ob solche Situationen vorliegen und wie ihnen zu begegnen ist, kann Gegenstand von Aufgaben eines Informatik-Revisors sein.

Grundsatz 9: Vertrag

Es bleibt mir an dieser Stelle nur, nochmals auf die Checklist der IG zu verweisen (siehe Endnote 4).

Berichterstattung und Ausnahmen

Da es sich bei der Auslagerung von Informatik bei Dienstleistungserbringern um technisch anspruchsvolle Gegenstände handelt, ist der Informatik-Revisor prädestiniert, eine entscheidende, wenn nicht federführende Rolle zu spielen.

Schlussbemerkung

Das RS scheint zwar noch einzelne Unklarheiten, praktisch kaum zu realisierende Forderungen und unterschiedlich interpretierbare Elemente zu enthalten, ist jedoch unzweifelhaft ein Schritt in die richtige Richtung. Die eidg. Bankenkommission hat mit dem RS eine Grundlage geschaffen, die dem Informatik-Revisor ein arbeitsreiches und anspruchsvolles Tätigkeitsfeld definiert. Eröffnet war es zwar schon lange, jedoch wurde ihm nicht immer die gebührende Aufmerksamkeit zuteil.

Max F. Bretscher, KPMG Fides Peat, Zürich

Endnoten

1 Rundschreiben der Eidg. Bankenkommission: Auslagerung von Geschäftsbereichen (Outsourcing) vom 26. August 1999

2 Control Objectives for Information and Related Technology © ISACF, Rolling Meadows, Illinois USA

3 IS Auditing Guideline effective September 1, 1999 © ISACA, Rolling Meadows, Illinois USA

4 Verfügbar via ISACA (Switzerland) Chapter home page http://www.isaca.ch/

5 Z.B. gemäss Bankenverordnung über die Banken und Sparkassen des eidg. Bundesrates, Stand 2. Dezember 1996, Art 44 Buchst o

6 Schweizerische Treuhandkammer: Grundsatz zur Abschlussprüfung Nr. 4, Arbeit eines andern Prüfers

7 American Institute of Cerified Public Accountants (AICPA): Statement on Auditing Standards 70 Reports on the Processing of Transactions by Service Organizations

Externalisation Commentaires sur la circulaire 99/2 de la CFB

L’importance de l’informatique pour les établissements bancaires rend quasi automatique l’application de la circulaire à toute activité informatique externalisée.

Seule une analyse détaillée des liaisons informatiques permettra d’évaluer le degré d’externalisation des processus informatisés et les risques liés à cette externalisation. Cette analyse doit être globale, puisque le réviseur doit s’assurer de la continuité des différents systèmes de contrôle interne. Un examen attentif des contrats permettra en outre de déceler les éventuelles incohérences entre les compétences et les responsabilités respectives des deux partenaires.

La checkliste établie par le groupe “IG outsourcing” de l’ISACA ainsi que le modèle de référence CobiT sont des outils indispensables à l’audit dans le domaine de l’externalisation de l’informatique. La vérification de l’application correcte de certaines dispositions, relatives par exemple à la confidentialité des données ou au transfert électronique des données à l’étranger, ne pourra être effectuée que par un auditeur informatique qualifié (CISA). Un travail intéressant en perspective!