Nr. 74 | April 2005

Schwerpunkt-Thema:

IT-Measurement

Inhaltsverzeichnis

Editorial 4

IT-Measurement – Performance Management in IT Security 6

IT-Measurement – Corporate & ICT Performance Management 8

IT-Measurement – Eine Retrospektive 11

Interviews 12

Outsourcing – Gartner Says 15

Projektcontrolling – Projektcontrolling von Migrationsprojekten im Bereich der IT-Infrastruktur 16

Audit Software – Datenprüfung im Werkzeugkasten der Revision 22

Express Line 27

The ISACA Crossword Puzzle 28

DACH-News 30

Veranstaltungen 33

Vereinsadressen 35

Impressum

Herausgeber:
ISACA Switzerland Chapter
c/o Monika Josi
Novartis Animal Health
Global Information Technology
WRO-1032.1.90
4002 Basel

Redaktion:
Max F. Bretscher
KPMG Fides Peat
Badenerstrasse 172
8026 Zürich
mbretscher@kpmg.com

Satz und Gestaltung:
WissensTransfer
Francesca Lüscher Baglioni,
8235 Lohn, SH

Jeder Nachdruck, auch auszugsweise, sowie Vervielfältigungen oder sonstige Verwertung von Texten oder Abbildungen aus dem ***NewsLetter*** nur mit schriftlicher Genehmigung des Herausgebers unter voller Quellenangabe.

Preise:
Mitglieder gratis
Abonnement CHF 35.–/Jahr
Einzelnummer CHF 10.–

Inserate:
1 Seite CHF 400.–
1/2 Seite CHF 240.–
1/4 Seite CHF 160.–

Erscheint 5 Mal jährlich
Auflage: 1350 Exemplare

Nächste Ausgabe (Thema: Biometrie):
Juni 2005, Redaktionsschluss: 20. Mai 2005

Editorial

Diese Ausgabe befasst sich mit der Produktivität und Leistungsmessung der Informations- und Kommunikationstechnologie (ICT). Bei der Produktivität geht es dabei um die Frage, welche Rolle die ICT bei der Steigerung der Wertschöpfung im Unternehmen spielt. Die Schweiz steht in der Anschaffung von ICT im Vergleich zu anderen Ländern an der Spitze. Schaut man aber auf die Anwendung, stellt man fest, dass sie oft nicht effizient genutzt wird. Bei der ICT besteht noch immer die Mentalität, die man folgendermassen umschreiben könnte: „Hier ist die Lösung – wo ist das Problem, Kunde?“

Lange Zeit wurde in Statistiken die ICT nirgends unter Produktivität ausgewiesen. Seit einem Jahrzehnt nun beginnt sie in den Vereinigten Staaten aufzutauchen. Es wird offensichtlich, dass die Komponente „Nutzung der ICT“ beinahe die Hälfte der Ertragskraft der USA ausmacht. Die Zeitschrift ***The Economist*** hat im Jahr 2004 eine Untersuchung veröffentlicht, in der die ICT als wichtiger Akteur in Bezug auf die Produktivität in Europa genannt wird. Darin zeigen sich grosse Unterschiede zwischen den nördlichen und südlichen Ländern Europas. In diesem Klassement befindet sich die Schweiz erstaunlicherweise am Schluss.

Wie können die Möglichkeiten, die neue Informations- und Kommunikationsmittel bieten, besser genutzt werden, um die Effektivität und Effizienz zu steigern? Eine Lösung, die sich immer deutlicher abzeichnet, ist das Konzept der „Transformer“. Neu daran ist, dass Unternehmer dank ICT effiziente Hilfsmittel zur Verfügung haben, mit welchen die Arbeitsabläufe, die Dienstleistungen und die Produkte rasch umgestaltet werden können. Die Transformation äussert sich gewissermassen in der „Software“ des Unternehmens. All diese Prozesse bilden ein Modell, das die Wertschöpfungskette erweitert und den Konsumenten bzw. Kunden besser einbezieht.

Als zweiter Lösungsansatz sollten die Leistungen entlang der Wertschöpfungskette transparenter gemessen und zielorientiert „gemanaged“ werden. Dieses Modell beginnt in der Wirtschaft vermehrt Fuss zu fassen. Mit den steigenden Anforderungen (Markt, Wettbewerb, Risiko, Rendite, Gesetz, Aufsichtsbehörde, Stakeholder) sind verlässliche Entscheidungsgrundlagen auf strategischer und operativer Ebene mehr denn je gefragt.

Die Hersteller von integrierten Business Intelligence (BI) Systemen geben sich alle Mühe, dafür ausgereifte Tools auf den Markt zu bringen. Um den gestellten Anforderungen gerecht zu werden, müssen BI-Plattformen fähig sein, Unternehmensdaten aus den verschiedensten Datenquellen zusammenzuführen, zu analysieren und auszuwerten.

Auf der neuen BI-Plattform sind Enterprise Reporting sowie Performance Monitoring vereint, welche die Basis für das Corporate Performance Management (CPM) und das ICT Performance Management bilden. Ausserdem sorgt die BI-Lösung dafür, dass mit visuellen Indikatoren, wie Charts, Pegelinstrumenten, Symbolen und Piktogrammen massgeschneiderte Scorecards und Dashboards erstellt werden können.

Einer Umfrage der Gartner Group zufolge sind die BI-Budgets in letzter Zeit weltweit deutlich gestiegen. Bekannte BI-Produkte werden laufend zu eigentlichen BI-Suiten weiter entwickelt. Die bekanntesten Hersteller sind: Cognos, IBM & SAS Institute, Oracle, Information Builders, Hyperion, Business Objects, Microstrategy. Um näher an die Kunden heranzukommen werden die BI-Anbieter im Verlaufe dieses Jahres in Deutschland, Österreich und in der Schweiz noch weitere Niederlassungen aufbauen. Laut den jüngsten BI-Trends sollen bereits komplette BI-Lösungen auch für kleine und mittlere Unternehmen mit einer Authoring-Lizenz von CHF 10’000 zur Verfügung stehen.

Die geforderten Ansätze haben weitreichende Auswirkungen auf die Steigerung der Produktivität der Mitarbeitenden und die Ertragskraft der Unternehmen. Diese so genannten Value-added-Services werden die Wirtschaft hinsichtlich Effizienz und Effektivität entscheidend beleben.

Wie Sie bereits bemerkt haben, hat sich mit Beginn des neuen Jahres das Design des ***NewsLetters*** verändert. Ich rege Sie dazu an, Ihren Feedback bezüglich Aufmachung und Inhalt der Redaktion zukommen zu lassen, damit wir Ihren Wünschen mit allfälligen Verbesserungen entsprechen können. Auch auf Ihre Beiträge in Form von Artikeln oder Referaten (u.a. ISACA ***NewsLetter*** oder ***After Hour Seminare***) würden wir uns besonders freuen. Nutzen Sie diese Inspiration als Chance für Ihren persönlichen Erfolg.

Bruno Wiederkehr

Editorial

Le thème de ce numéro: la productivité et la mesure des performances dans le domaine informatique. Les statistiques publiées récemment montrent que la Suisse investit très largement dans les technologies de l'information. La contribution de ces investissements à l'augmentation de la productivité reste cependant en rade. Ne sommes-nous peut-être pas assez critiques par rapport à l'approche des vendeurs : « excellente solution, cherchons le problème ! »

La prise en compte de la contribution de l'informatique dans les statistiques de productivité n'a démarrée qu'il y a quelques années aux Etats-Unis. Il apparaît qu'aujourd'hui la moitié de la hausse de productivité des USA est à mettre au compte de l'informatique. Les chiffres publiés en 2004 par ***The Economist*** confirment l'importance de ce facteur informatique pour l'Europe mais montrent également le fossé séparant le Nord et le Sud de l'Europe. La Suisse figure en queue de peloton.

Comment mieux mettre à profit le potentiel offert par les nouvelles technologies pour augmenter la rentabilité et l'efficacité de la gestion? Une des solutions souvent évoquée : le concept « transformer ». L'entreprise saisit l'occasion de se transformer en s'appuyant sur les nouveaux outils mis à disposition par les technologies de l'information. Cette transformation s'exprime dans tous les processus et dans le « software » de l'entreprise. La chaîne de valeur ajoutée peut ainsi être adaptée dans une perspective d'amélioration du service à la clientèle.

La seconde piste à suivre est la mesure systématique des prestations tout au long de la chaîne de valeur ajoutée. Cette démarche implique une transparence qui semble de plus en plus souhaitée par les directions d'entreprises. Ces dernières ont en effet besoin d'informations fiables leur permettant de prendre les décisions correctes pour faire face à l'évolution des marchés, de la concurrence, des risques, des besoins des clients, de la technologie ou des autorités de surveillance.

Cette évolution ouvre un nouveau marché aux fabricants d'outils d'intelligence artificielle (BI). Pour réussir à placer leurs produits, ceux-ci doivent être en mesure de consolider puis d'analyser sur une plateforme unique des données provenant d'environnements souvent très hétéroclites et non standardisés.

Au nombre de ces nouveaux logiciels les Enterprise Reporting ou Performance Monitoring qui permettent un Corporate Performance Management (CPM) ou un ICT Performance Management. Les méthodes de présentation doivent être concises et recourent fréquemment aux outils graphiques déjà connus dans le domaine des tableaux d'indicateurs et des Scorecards.

Selon une étude récente du Gartner Group, les budgets consacrés à la BI ont considérablement augmenté ces dernières années. Ils sont souvent regroupés dans des BI Suite. Il semblerait que les modèles de base permettant à une entreprise de démarrer dans ce domaine seront prochainement offerts à partir de 10'000 francs suisses. Les principaux fournisseurs sont aujourd'hui : Cognos, IBM & SAS Institute, Oracle, Information Builders, Hyperion, Business Objects, Microstrategy.

Il reste à espérer que toutes ces initiatives auront une influence positive sur la productivité des entreprises et de leurs collaborateurs !

Vous avez certainement remarqué que votre ***NewsLetter*** a fait peau neuve. La rédaction est toujours intéressée par vos commentaires et vos propositions. D'une manière générale, n'hésitez pas à nous contacter si vous avez des idées d'articles ou de présentations dans le cadre des ***After Hour Seminare***). Une manière de partager votre savoir et de contribuer à votre développement personnel !

Bruno Wiederkehr

2005 Jahr der Technik

Die ISACA unterstützt als teilnehmender Partner das nationale „Jahr der Technik" 2005 – Eine Initiative zur Stärkung des Technik- und Innovationsstandortes Schweiz unter dem Patronat von Bundesrat Joseph Deiss.

IT-Measurement

Performance Management in IT Security

The following article is based on an interview conducted with James Gurney, Novartis Consumer Health Global Information Security Officer. James Gurney is currently working toward a PhD in Information Security Management with an emphasis on measuring ISEC performance in objectives, dollars and sense. His research for the PhD is a collaboration between Novartis and the University of Geneva and was brought on by his dissatisfaction with the real lack of Performance Management in information security. The idea came about through recent studies for the CISSP (Certified Information Systems Security Professional) qualification.

Questions

Current Situation

■ What is the goal of Performance Management in IT Security?
The goal of Performance Management in Information Security is to provide the tools and mechanisms for an organisation to specify, collect and monitor measurement criteria in order to enable improvement of Information Security over time. Such information will then arm the IT and Information Security professional with the ability to identify year-on-year measurable criteria with which to manage their function.

■ How are Performance Management Criteria for Information Security implemented across industries today?
Very few organizations actually have a Performance Management Program directly related to Information Security today and this is one of the key drivers behind my work. Many organisations are attempting to measure the effectiveness of Information Security through audit results, limited event reporting or static related performance criteria gauging for example user or employee awareness of Information Security.

■ Are there already 'good practice' Criteria out there?
I believe that at the moment any Performance Management practice is good practice within reason. However, many of the most interesting initiatives in this field are still very much within the research environment with the exception of a few consultancies who claim to offer „Performance Management Solutions" for their clients. But these solutions tend to consist of the same old KPIs and risk assessment scores that most of us are already aware of and have implemented.

Problems and Implications

■ What are the problems and their implications to the companies derived from the current status?
Clearly the risks related to information security as threats become evermore elaborate. Under these auspices we can assume that greater focus is required on security than at present in order to be able to manage these risks. Combine this situation with the ever increasing financial restraints that organizations are under and the fact that management are constantly looking for ways to measure and consequently improve performance and we arrive at the basic need for Performance Management in Information Security. Despite the high profile associated with Information Security incidents in recent years, management awareness of Information Security could be much greater and consequently the support for ISEC activities within organizations could be radically improved. So in essence, despite the huge advances in Information Security activities and provision, I still believe that more commitment and buy-in is required and an effective way to achieve this will be to professionally demonstrate the performance and benefits of security within the organisation.

■ How could Performance Management Criteria be defined?
A very good question that I am still in the process of trying to answer. Basically the idea behind Performance Management and Benefits Realisation in Information security is to investigate ways in which we can measure and meaningfully represent the worth of our efforts over time. There are various ways in which I hope we will be able to make improvements in the future. These include :
– Value Measurement: There are many ways in which we could measure the true value of Information Security and understand the benefits in financial and other measurable terms.
– Expenditure: On the whole we are currently limited to a historical analysis of Information Security expenditure, which can be compared to prior years. Current research into Return on Investment (ROI) within security will help us to get a better financial understanding of the costs and benefits.
– Comparison: Current benchmarking activity for Information Security is very limited. There are some private companies and institutions gathering benchmark information but these activities are not particularly widespread. Furthermore, the type of benchmark criteria currently collected are subject to the kind of limitations

mentioned earlier. Basically, this information is not enough to move information security forward in real business terms.

– Performance Measurement: Currently nothing adequately addresses the quantitative benefits of information security with the exception of motoring project and progress milestone measurements. Further and deeper analysis of performance benefits in terms of the allocation of resources will better enable us to understand the delivery of security activities and make proactive improvements.

– Uncertainty: Scenarios within Risk Management currently address, in a qualitative manner, the uncertainty of threat. I believe that such scenarios can perceivably be measured in more tangible business terms such as the possible saving of resources or such as time and money. Clearly a tenuous measurement at first glance and certainly the most creatively challenging aspect of my work at the moment. But I believe that time, work and good consultation will deliver some interesting results in respect of these ideas.

The difficult problem is which measurements to investigate as there are some many aspects to security (and control) that could effectively be measured, monitored, assessed and ultimately add value to information security and the mission of an organisation.

■ How could they be collected?

This is all a question of management and sound methodology. While I consider information gathering to be one of the lesser intellectually challenging areas of this project, it remains an essential element that will assist information security practitioners and ultimately add value to the organisation.

■ Will they be industry-specific or generally applicable?

Another very interesting question (meaning that I don't have a clear answer!). Risk scenarios obviously differ across industry sectors as do the essential drivers for information security such as regulatory compliance for example and the nature of an organisations information assets with consideration to Confidentiality, Integrity and Availability. The value proposition of the organization will also be key to the requirement for ISEC Performance Management and ultimately impact the aforementioned ISEC drivers. My current approach is to remain all-encompassing in terms of what this project will deliver in order for the outcome to be as useful to a public sector organization as it would be to a bank.

Benefit

■ What will be the benefit for the companies applying such Criteria?

Firstly, the ability to better understand how resources allocated to Information Security perform, set clearer objectives and help make improvements over time. Couple this with the ability to better communicate performance, value and improvements over time in true business terms and the benefits are clear.

■ Will they actually provide information to the companies regarding areas for improvement?

I certainly believe so, but implementation will be the key to everything. It is my aim to pilot the results of my research before publishing and hopefully to remain available to help and advise those organisations who put the methodology into practice. With improvement as the main goal, effective implementation will almost certainly help organisations to improve Information Security performance over time.

■ When will your work be available? Will this be openly available?

I intend to publish two papers, one in 2005 and one in 2006 when I also plan to complete this project and write a thesis. As this is a serious research project between The Universty of Geneva and my company, my work will ultimately generate a published thesis, which will be publicly available.

James Gurney, Novartis Consumer Health, Basel

IT-Measurement

Corporate & ICT Performance Management

Das wichtigste Motiv für eine verbesserte Messung der Produktivität heisst „Veränderung". Angesichts des schnellen Wandels in der Wirtschaft werden die Geschäftsmodelle mit ihrer Informations- und Kommunikationstechnologie laufend an die neuen Herausforderungen angepasst. Nach Jahren hoher Kapitalüberschüsse und Investitionen sehen sich die Unternehmen zunehmend gezwungen, bei der Zuordnung des Kapitals zu den einzelnen Geschäftsfeldern „mit spitzem Stift" zu rechnen. Alle wollen Kosten senken, Risiken minimieren, Gewinne steigern und die Verantwortlichkeiten optimal organisieren. Aber wie soll das funktionieren?

Ein unternehmensweites Performance Management bietet die Lösung. Nachhaltiger wirtschaftlicher Erfolg setzt heute ein unternehmensweit konsistentes Führen und Steuern von Teams, Prozessen und Systemen in einem dynamischen Umfeld voraus. Corporate Performance Management (CPM) definiert den Anspruch, die Leistungsfähigkeit über alle Unternehmensbereiche und den gesamten Managementzyklus zu überwachen. Das Ziel ist, alle operativen Massnahmen (auch die der ICT) optimal auf die Unternehmensstrategie abzustimmen und ihre Auswirkung auf das Geschäftsergebnis transparent zu machen.

Zwar zählt die Schweiz in Sachen ICT-Investitionen weltweit zu den Spitzennationen. Bei der daraus resultierenden Produktivität gehört sie aber zu den Nachzüglern. Xavier Comtesse, Autor von Dartfish, hat dies entsprechend in der Publikation von Avenir Suisse festgehalten. Weiter wurde vermerkt, dass die Firmen zwar enorm Technik-begeistert sind, sie jedoch nicht recht wüssten, wie die moderne ICT einzusetzen sei, um die Produktivität zu steigern. Ob dies wohl in der mangelnden ICT-Strategie oder in der stetigen Anschaffung von Hightech Neuheiten ohne definierten Verwendungszweck liegt?

Wie bereits im Editorial erwähnt, gibt es verschiedene Ansätze, die zu einem Produktivitätsgewinn führen. Auf allen Hierarchieebenen sollte sich die Erkenntnis durchsetzen, dass die Produktivität nicht nur von den ICT-Investitionen abhängt, sondern auch vom gezielten Einsatz der Anwendungen und insbesondere von den Leistungsfaktoren entlang der gesamten Wertschöpfungskette. Ich schlage vor, von einem technischen Perfektionismus wegzukommen, die Business- bzw. ICT-Entwicklungen in guter Zusammenarbeit mit dem Kunden zu fördern – „der Kunde ist König" – sowie die Leistungen beider Partner zu messen.

Anlässlich eines nächsten ISACA After Hour Seminars wird zum Thema CPM ein Überblick über diese Managementphilosophie und die Leistungsmessung mittels BI präsentiert. Es wird dabei auf die Möglichkeiten eingegangen, wie die Steigerung der Produktivität des Unternehmens durch die ICT- und die Audit-Funktion unterstützt werden kann.

Wichtige Einflussfaktoren

Zunehmend komplexer werdende Business-Anwendungen sowie der Druck von Seiten der Stakeholders und Aufsichtsbehörden zwingen die Unternehmen, ihr Kapital-, Risiko- und Performance-Management zu verbessern. Ein Erfolg ist nur möglich, wenn eine entsprechende Kultur vom Verwaltungsrat und dem Management vorgelebt wird und in sämtlichen Geschäftsprozessen verankert ist.

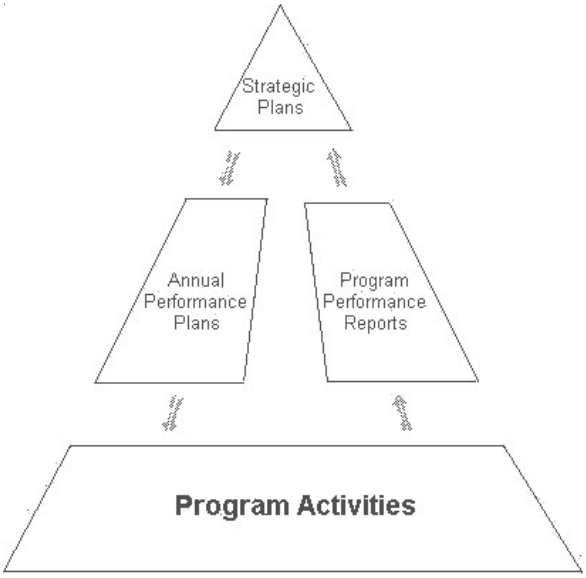
Impulse zum Wandel

Der Schlüssel zum Erfolg liegt in der Information und der Kommunikation. Es muss allen Parteien klar und verständlich sein, was das Unternehmen erreichen will. Das Wissensspektrum reicht von der Vision über die Strategie des Managements bis hin zur Mission, die den Mitarbeitenden erklärt, wozu sie berufen sind und welche Leistungen von ihnen erwartet werden.

Der President's Message vom ISACA Global Communiqué 1/2005 ist zu entnehmen, dass zwischen der Effektivität und Messbarkeit von IT Governance sowie der Frequenz, mit welcher die IT auf Verwaltungsratsebene diskutiert wird, ein Zusammenhang besteht. Von Unternehmen, bei denen ICT ständig auf der Agenda steht, wurden folgende Hauptthemen der IT/ICT als verbesserungsfähig erklärt:

- Alignment of IT with the company strategy
- Delivery of business value through IT
- Management of IT ressources
- Management of IT risk
- Measurement of IT performance.

Mit der folgenden Graphik wird das Zusammenspiel der einzelnen CPM Elemente dargestellt.



Alignment of Strategic & Performance Plans

Modelle und Ansatzpunkte

Unternehmer und Stakeholder haben erkannt, dass es in den Bereichen Finanzen, Verwaltung, Rechnungswesen und ICT noch Potenziale für Effizienzsteigerung und Kostensenkung gibt. Anerkannte Modelle zur Leistungsmessung und Steigerung der Produktivität stehen bereits heute zur Verfügung. Das Wissen darüber sollte in die Grundlagen der Gegenwart integriert und angewendet werden, damit die richtigen Entscheidungen hinsichtlich Risiken, Leistungen, Qualität und Erfolg getroffen werden können. Zudem wird vom Management in immer kürzeren Intervallen eine möglichst schnelle und konsistente Berichterstattung darüber erwartet.

In vielen Unternehmen werden bekannte Modelle, Standards und Guidelines noch nicht oder zu wenig konsequent eingesetzt und adäquat angewandt; wie z.B.:

- IT Governance Implementation Guide – www.itgi.org
- CobiT Framework mit Bezug auf IT Prozesse, IT Ressourcen & Informationskriterien (z.B. Effektivität & Effizienz) – www.isaca.org
- IT Performance Management (inkl. Balanced Scorecard) – www.isaca.org/knet & www.gao.gov
- IT Management Guidelines mit Bezug auf Key Performance Indicator & Benchmark – www.isaca.ch
- Business Intelligence (BI-integrierte Werkzeuge inkl. Scorecarding) – www.cognos.ch

Umsetzung und Erkenntnisse

Als wesentlich sind bei der Umsetzung die Erkenntnisse und Erfahrungen aus der Vergangenheit zu betrachten. Im Mittelpunkt stehen immer noch die Mitarbeitenden mit ihren Vorstellungen, welche die Veränderungen der Unternehmen realisieren oder blockieren. Heutige BI-Werkzeuge machen es möglich, zielorientierte Kennzahlen von jedem Arbeitsplatz abzurufen. Gleichzeitig können Unternehmensziele mit Leistungen und Verantwortlichkeiten der Mitarbeitenden verknüpft werden. Durch die Erstellung, Analyse, Präsentation und Verteilung von zeitkritischen Informationen können – ausgehend von der Strategie – die notwendigen Entscheidungen rechtzeitig getroffen und Aktionen eingeleitet werden.

Aus der nebenstehenden Graphik sind die einzelnen Elemente des CPM Lebenszyklus' ersichtlich.

Wenn es gelingt die Mittel, Methoden und Verfahren gezielt einzusetzen sowie aktiv und intensiv den Wandel zu beschleunigen, ist man der konstruktiven Messung von Leistungen sowie der Verbesserung der Produktivität einen Schritt näher gekommen.

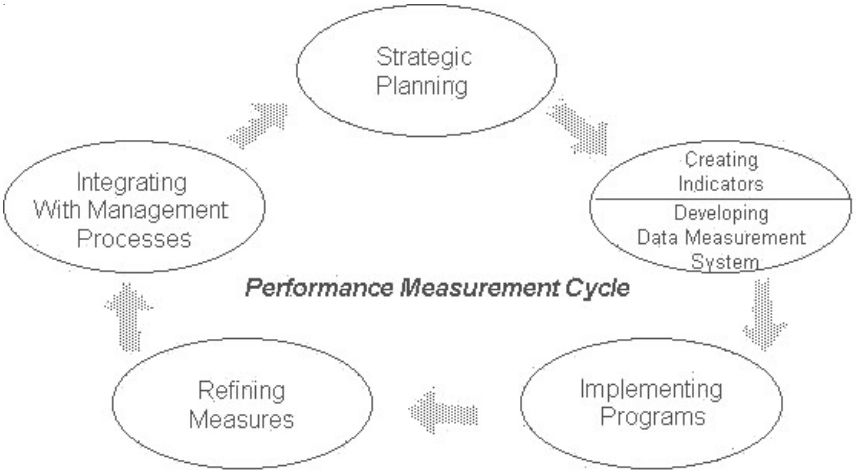
Rolle der Audit-Funktion

Eine modern ausgestaltete interne und externe Revision kann dazu beitragen, dass die Verantwortung von CPM als Voraussetzung wahrgenommen wird. In diesem Zusammenhang stellt sich die Frage, was der Revisor zur Steigerung der Effizienz und Effektivität bzw. Produktivität der ICT beitragen kann.

Mit der Beherrschung von Revisionsgrundsätzen verfügt ein Revisor in grossem Masse über das Wissen und die Fähigkeiten im Zusammenhang mit CPM. Um mit der ausreichenden Qualifikation zu überzeugen, sind Ausbildungslücken bezüglich CPM zu schliessen. Im Bereich BI können Zertifikate als Certified Business Intelligence Professional beim Institut for Certification of Computing Professionals – www.iccp.org – abgeschlossen werden.

Wird jedoch die Kosten-Nutzen-Relation vermehrt in die Aufgabenerfüllung des Revisors einbezogen, können mit der Beurteilung der Produktivität und korrekten Leistungsmessung seine Ergebnisse verbessert und mögliche Chancen leichter erkannt werden.

Mit Kennzahlen, Geschäfts-, Budget- und Informatikinformationen kommen die meisten Information Systems Auditoren mit der alltäglichen Praxis



in Berührung. Zur Beurteilung wird empfohlen, vermehrt die bestehenden Standards und Guidelines sowie das CobiT-Framework (u.a. Management Guidlines, Balanced Scorecard) konsequent einzusetzen. Mit der Kombination anerkannter Audit-, Management- und Überwachungs-Instrumente werden die Interessen der Geschäftsleitung geweckt und durch realisierte Chancen die Akzeptanz der Revision gestärkt.

Fazit

Die geforderten Veränderungen haben eine weitreichende Auswirkung. Die ICT soll effizient und kundenorientiert das Business unterstützen. Sie hat sich an der Geschäftsstrategie auszurichten und muss – last but not least – wirtschaftlich sein.

Wer die Zeichen der Zeit erkannt hat und sich gedanklich wie praktisch der Leistungsmessung und -beurteilung stellt, wird auch in Zukunft Erfolg haben. Durch Inspiration und Kommunikation kann die Lebenskraft und damit die Leistungsfähigkeit der Mitarbeitenden gesteigert werden. Das kommt letztlich wieder dem Geschäftserfolg zu Gute. Dabei kann der ICT-Revisor mit seinen umfassenden Wissen, Hilfsmitten und Informationen einen wesentlichen Beitrag leisten.

Motto: You cannot manage what you cannot measure. Dies verpflichtet auch von einem Performance „Measurement“ zu einem Performance „Management“ überzugehen.

Bruno Wiederkehr
ICT Consulting & Training

IT-Measurement

Eine Retrospektive

In den späten sechziger Jahren des vergangenen Jahrhunderts wurden diverse Dissertationen und sogar Habilitationen zum Thema der Verrechnung von Computerleistungen geschrieben. Ich selber erlebte hautnah die Streitereien über das Verrechnen von Input-Output-Aktionen, Zentralrechner-Sekunden, Beanspruchung von Magnetbändern und Diskplatzbelegung. In jenen Zeiten kostete ein Kilo Computer mehr als ein Kilo Gold. Es ist deshalb verständlich, dass die Verrechnung der abzuschreibenden Millionen ein heiss umstrittenes Thema war.

Angestrebt wurde eine gerechte Verrechnung der Computerleistungen an die Benutzer. Die Gehälter für die Bediener (Operators) könnte man zwar als variabel deklarieren, doch gab es schon damals wenig Computer-Tätigkeiten, welche von der Anzahl Bediener abhängig waren. Somit war ein riesiger Klumpen Fixkosten vorhanden, der auf die Benutzer umzulegen war. Die meisten Inhaber/Benutzer von Grossanlagen lasteten die Kosten arbiträr den bestverdienenden Abteilungen (oder jenen, die man loswerden wollte) an. Da die zu ergatternden Boni von der monetären Situation unter dem Strich (genannt Deckungsbeitrag) abhängen, wehrten sich die Belasteten umgehend, und jedermann erklärte sich bald berufen, ein „gerechtes“ System der Verrechnung von Computerleistungen zu präsentieren.

Besonders ausgeprägt stellte sich die Frage bei Dienstleistungs-Rechenzentren. Ausgeklügelte „Accounting-Systeme“ versuchten zu belegen, weshalb die erbrachten Leistungen „richtig“ waren. Nachprüfen konnte man sie ohnehin nicht. Einige Schlaumeier programmierten nutzlose Schlaufen in ihre Programme, damit mehr Zeit verbraucht wurde, und derart der Preis ihrer Produkte erhöht wurde.

Der Wert von Computerprogrammen wurde mit der Anzahl Programmzeilen gemessen, was dazu führte, dass auch hier Unfug betrieben wurde. Ein Statement wurde auf mehrere Zeilen verteilt und/oder wenig sinnvolle DO NOTHING Befehle fanden ihren Eingang in Computerprogramme.

Computer sind heute zu einem Preis zu haben, der tausendfach billiger bei gleichzeitig tausendfach höherer Computerleistung ist. Hardware ist eine beinahe vernachlässigbare Grösse in der Verrechnung geworden. Längst sind Betrachtungen pseudo-mathematischer Überlegungen bezüglich messbarer Computereinheiten in Sekunden und Bits verschwunden. Es sind Elemente wie Verfügbarkeit und Reaktionszeiten (von Antwortzeiten ganz zu schweigen), welche einen wesentlichen Einfluss auf den Preis haben, den ein Benutzer zu bezahlen bereit ist. Wie misst man heute die IT-Leistungen?

Input-Output-Aktionen, Benutzter Speicherplatz und Zentralrechnersekunden sind exakt messbar, die heute gefragten Leistungen weniger. Das geflügelte Wort, dass nur beherrscht werden könne, was messbar ist, weist einen beschwerlichen Weg. Wenn heute das Bereithalten der Information und die erfolgte Kommunikation ausschlaggebende Charakteristika der IT sein sollen, müssen diese Elemente messbar gemacht werden. Wie ist z.B. die riesige Informationsmenge einer Google-Datei (inklusive der ausschlaggebenden Suchmaschine) zu bewerten und zu messen?! Wie ist die Qualität einer Workhouse-Datenbank zu bemessen? Was soll den Wert eines Computerprogramms bestimmen?

Zugegeben, einzelne Elemente, wie Downtime eines Systems, Antwortzeiten, Turn-around-Zeiten usw. lassen sich vorgeben und messen, bei anderen habe ich meine Zweifel. Dies ist insbesondere dann der Fall, wenn qualitative Faktoren ins Spiel kommen. Ich betrachte dies als die grösste Herausforderung an die IT-Betreiber und -Messer der heutigen Zeit. Inwiefern die IT-Revisoren in der Lage sind, einen wesentlichen Beitrag bei der Definition und der Messung von IT-Leistungen zu leisten, wage ich nicht zu beurteilen. Aber eine Herausforderung wären die Aufgaben sicher.

Max F. Bretscher

Interviews

François Vaillant

Directeur Audit des Systèmes d'Information, Groupe Accor

„Le métier de l'audit des systèmes d'information a fortement évolué"

Avec plus de 150 000 collaborateurs dans le monde et près de 7 milliards de chiffre d'affaires en 2003, le Groupe Accor est axé autour de deux grands métiers : l'hôtellerie et les services aux entreprises & collectivités. Son Directeur audit revient sur son parcours et les spécificités de sa fonction.
08/10/2004

Emploicenter. Pourriez-vous nous résumer en quelques mots votre parcours ? Comment êtes-vous arrivé à l'audit ?

François Vaillant. J'ai débuté ma carrière en 1989 chez PricewaterhouseCoopers et j'y suis resté près de 7 ans, atteignant la qualité de manager. J'ai ensuite intégré l'audit interne du Groupe Bull, en charge de l'audit informatique, puis de la direction de projets européens d'infogérance. Début 1998, j'ai eu l'opportunité d'intégrer le Groupe Accor pour créer, animer et développer la Direction de l'Audit des Systèmes d'Information au niveau mondial. Je suis pleinement à cette tâche depuis plus de 6 ans.

Parallèlement, j'ai obtenu en 1996 la certification CISA et j'ai intégré en 2000 le conseil d'administration de l'Association Française de l'Audit et du Conseil Informatique, commission Formation. Dans ce cadre, nous avons mis en place un partenariat avec l'Université Paris Dauphine et nous avons créé en 2001 un DESS d'Audit et de Conseil en Systèmes d'Information, ce qui m'a amené à enseigner.

Vous orienter vers l'audit informatique, c'était un choix ou un hasard ?

Je suis arrivé dans l'audit informatique par hasard, comme beaucoup d'autres à cette époque. Il y a quinze ans il n'y avait pas de formation qui préparait à cette profession, encore assez confidentielle – les formations dédiées restent d'ailleurs très peu nombreuses aujourd'hui. Après mes études, je souhaitais être rapidement en contact avec des clients, de préférence multiples et variés en termes de secteur d'activité. PwC m'a donné cette opportunité.

„Nous intervenons sur les outils informatiques, les organisations et les processus"

Quelles sont vos principales missions au sein d'Accor ?

D'abord, notre démarche est critique par nature mais doit être avant tout constructive et ne peut donc se concevoir que dans le cadre d'un réel partenariat avec les directions opérationnelles et la Direction des Systèmes d'Information.

L'audit informatique de conformité est encore embryonnaire au sein du groupe. Notre démarche s'inscrit davantage dans le registre de l'audit d'efficacité et d'accompagnement, plus opérationnel et porteur de valeur ajoutée. Nos interventions couvrent les outils informatiques, les organisations et les processus et s'articulent autour de 4 grandes familles : audit d'organisation et de performance de la fonction informatique, audit de projet, audit d'applications et de processus informatisés et audit de la sécurité des systèmes d'information.

Comment définiriez-vous votre métier ? Quelle conception en avez-vous ?

Ce métier a fortement évolué. Né avec le développement de l'informatique dans le domaine de la gestion comptable et financière, il s'apparentait à l'origine à une fonction de support à l'audit financier. On parlait alors d'audit ou de révision en milieu informatisé. Au fil des ans, l'audit des systèmes d'information s'est professionnalisé, a élargi son spectre de compétences et son périmètre d'intervention, ce qui lui a permis de s'affirmer progressivement comme une discipline à part entière et d'acquérir une véritable légitimité dans l'entreprise. Sa mutation n'est toutefois pas achevée et son image reste parfois brouillée entre ses dimensions de contrôle et de conseil.

„La plus grande frustration pour l'auditeur est la non mise en œuvre de ses recommandations"

Quels sont les avantages et les possibles inconvénients de ce métier ?

Les avantages sont multiples : variété des sujets et des missions, vision étendue de l'entreprise et de son mode de fonctionnement, contacts fré-

quents avec la Direction Générale… Ce métier procure également à l'auditeur, et principalement à l'auditeur interne qui inscrit sa démarche dans la durée, de grandes satisfactions et notamment celle de voir appliquer avec succès ses recommandations et d'en mesurer ensuite les effets, ce qui permet de valider la pertinence du diagnostic et la justesse des recommandations. Inversement, la plus grande frustration de l'auditeur est la non mise en œuvre de ses recommandations.

Quelles sont vos méthodes de travail ?

Nous avons bâti nos propres référentiels et développé des outils et des méthodes, adaptés au Groupe et à son secteur d'activité. Ce travail s'est bien entendu inspiré des référentiels nationaux et internationaux reconnus tels que COSO, COBIT, ITIL, CMM, Marion…

Comment est constituée votre direction ?

La Direction de l'audit des systèmes d'information est rattachée à la Direction financière du Groupe, elle-même rattachée au Directoire. Ce rattachement est adapté et offre une grande indépendance vis-à-vis de la DSI du Groupe. D'autres organisations sont néanmoins possibles. Elle est composée de 5 collaborateurs pour couvrir l'ensemble des divisions et des pays du Groupe. Je m'appuie sur 2 Managers qui ont entre 8 et 10 ans d'expérience dans l'audit des systèmes d'information, et sur 2 seniors confirmés disposant d'environ 4 à 5 ans d'expérience. Les missions sont réalisées en binôme, 1 manager et 1 senior, et j'en assure la supervision.

Existe-t-il un profil type d'auditeur informatique ? Quelles qualités faut-il avoir pour exercer ce métier ?

Il n'existe pas de profil type : une formation Bac + 4 ou Bac + 5 dans le domaine des systèmes d'information permet un apprentissage plus rapide du métier mais des formations en école de commerce ou MSG ne sont pas incompatibles avec l'exercice de la profession, à condition d'être passionné par l'informatique et d'effectuer un travail personnel important dans ce domaine. A noter d'ailleurs que nous retenons à l'Université Paris-Dauphine presque autant de candidats diplômé de MSG que de Miage au sein du DESS. Les qualités et les compétences requises sont en revanche nombreuses : un bon background technologique est bien sûr indispensable pour être crédible vis-à-vis de la DSI, mais l'auditeur IT doit en outre être doté d'une bonne culture générale, économique et financière notamment, et d'une bonne sensibilité métier. Sans caractère d'exhaustivité, ses principales qualités seraient : la curiosité, l'intégrité, et bien sur de fortes capacités d'analyse, de synthèse et de conviction.

Est-ce qu'un passage en cabinet d'audit est obligatoire en début de carrière pour accéder à des postes en entreprise ?

Le passage en cabinet n'est pas obligatoire, mais facilite grandement l'accès à des postes d'auditeurs internes en systèmes d'information. Ainsi 100% des collaborateurs de mon équipe sont issus des grands cabinets anglo-saxons. Il est en effet plus difficile d'intégrer des juniors dans de petites structures et, jusqu'à présent, j'ai toujours privilégié des candidats immédiatement opérationnels.

Christian Masson

Responsable de l'Audit informatique, Banque de France

„Il faut être capable de convaincre les audités"

A 36 ans, Christian Masson évalue la qualité des dispositifs mis en place par les opérationnels de la Banque de France afin de contrôler les risques. Son programme annuel d'audit est validé par le Gouverneur de la Banque. 08/10/2004

Emploicenter. Pourriez-vous nous résumer en quelques mots votre parcours ? Comment êtes-vous arrivé au métier d'auditeur informatique ?

Christian Masson. De formation généraliste, je suis entré à la Banque de France par concours en 1994. J'ai opté pour un poste d'auditeur au sein de l'Inspection Générale. Mon rôle était alors davantage tourné vers l'organisationnel que vers l'informatique. J'ai ensuite occupé différents postes qui m'ont conduit vers ce que je fais actuellement. Je suis ainsi devenu chef de mission audit Informatique en 2002 avant de prendre la responsabilité du pôle en janvier dernier.

Comment est organisé votre service ?

L'Audit des Services Centraux est rattaché au Contrôleur Général. Il regroupe trois pôles, placés sous l'autorité d'un Directeur : l'Audit Général, l'Audit Informatique et l'Audit Comptable. Je suis responsable de l'Audit Informatique, qui comprend 2 chefs de missions et 5 auditeurs. Nous sommes indépendants des services que nous sommes amenés à auditer, et notamment de la Direction Infor-

matique qui, à la Banque, est constituée de deux entités : Organisation & Développement et Informatique & Télécoms.

Quelles sont vos principales missions ?

Nous avons quatre grands types de missions : des audits de projets, d'applications, de composants techniques et d'unités. Nous couvrons tout le système d'information de la banque. En tant qu'auditeur, nous évaluons la qualité des dispositifs mis en place par les opérationnels pour contrôler les risques. Notre programme annuel d'audit est validé par le Gouverneur de la Banque. Nous proposons ainsi deux ou trois audits de projets chaque année. Nous évaluons la qualité de la conduite de ces projets. Nos rapports contiennent des recommandations, auxquelles répondent les plans d'action des audités. Nous assurons par la suite tous les ans un suivi de ces plans pour mesurer leur avancement.

Quelles sont vos méthodes de travail ?

Nous appliquons les normes professionnelles d'audit de l'IIA et de l'ISACA. Pour l'évaluation des systèmes d'information, nous utilisons comme référentiel un certain nombre de règles édictées en interne ou des standards externes comme le CobiT.

Quelles qualités faut-il avoir pour exercer ce métier ?

Ce sont des qualités nécessaires pour tout auditeur : rigueur, sens de l'observation, qualités de communication et de rédaction. Le produit fini étant un rapport assorti de recommandations, il faut aussi être capable de convaincre les audités. Il faut enfin une certaine connaissance du domaine audité, et en l'occurrence de l'informatique même si nous ne sommes pas des techniciens. Tous nos chefs de mission et auditeurs sont ainsi certifiés CISA ; nous encourageons depuis plusieurs années l'inscription à cet examen. La pratique de l'anglais est également importante. La Banque de France fait partie du Système Européen de Banques Centrales et nous menons des missions d'audit conjointement avec la BCE et les autres Banques Centrales Nationales.

Repris avec la permission de L'AFAI

IT-Tagung 2005

Aktuelle Entwicklungen, Methoden, IT-Sicherheit, Tools und Technik

IIR Akademie

Vom **30.-31.Mai 2005** in Frankfurt

Themen:
- Risiken und Chancen von RFID Anwendungen für Datenschutz und Datensicherung unter Revisionsaspekten
- IT-Self Assessment: Ein innovatives Projekt der Rechnungshöfe in Europa
- Führt die Auflösung der Perimetersicherung zu Kontrollverlust?
- Penetrationstest als Revisionswerkzeug – Ein Motivationsversuch
- SSE-CMM – Ein Standard zur Reifegradmessung von IT-Security-Management-Systemen
- Datenschutzaudit - Anforderungen und Umsetzung in der Praxis
- Normen und Standards in mittelständischen Unternehmen
- VoIP – Audit und Sicherheit
- Vorstellung des ISACA Linux Audit Tools
- Forensische Datenanalyse
- Projektrisiko-Beurteilung - Planung der projektbegleitenden Revision

Weitere Infos unter:
Deutsches Instituts für Interne Revision e.V. (IIR)
Ohmstraße 59
60486 Frankfurt am Main
Telefon (069) 71 37 69-0
Telefax (069) 71 37 69-69
http://www.iir-ev.de

Outsourcing

Gartner Says

The worldwide market for customer service outsourcing is set to grow from $8.4bn in 2004 to $12.2bn in 2007, but the offshore component will remain small, according to Gartner Inc. Gartner research director Alexa Bona today presented „The myths and realities of customer service outsourcing" at its Customer Relationship Management Summit 2005 in London. The presentation identified business risks associated with customer service outsourcing, contradicted a number of misconceptions surrounding the dominance of offshore call centres and offered key recommendations to make customer service outsourcing pay. Key findings:

- The worldwide market for customer service outsourcing is set to grow from $8.4bn in 2004 to $12.2bn in 2007.
- Through 2007, 80 percent of organisations that outsource customer service and support contact centres with the primary goal of reducing cost will fail.
- Up to 2008, 60 percent of organisations that outsource parts of the customer-facing process will encounter customer defections and hidden costs that outweigh any potential savings they derive from outsourcing.
- Despite the hype surrounding offshore call centres, offshore customer service outsourcing only represents a tiny fraction of the market – less than 2 percent in 2005, increasing to less than 5 percent in 2007.
- By year-end 2005, 70 percent of the top 15 Indian owned BPO startups that offer customer call centre services will be acquired merged or be marginalised.
- Outsourced contact centres have higher staff turnover than in-house contact centres.

„Our research shows there are significant risks associated with outsourcing customer service," said Alexa Bona, Research Director at Gartner. „Historically, outsourcing has been seen as a way to reduce costs by getting others in cheaper locations, or with greater economies of scale, to own the processes that are not core to the business. Companies are encountering problems because they don't approach this strategically. They usually lack information to make meaningful cost/benefit analysis and often focus on inappropriate or unmeasureable service levels and cost metrics."

According to Gartner, companies that outsource successfully can achieve cost savings of 25 to 30 percent. However, Ms Bona warned that a poorly managed model can reduce the quality of the customer experience, dilute the brand values of the company and fail to deliver cost savings.

Ms Bona went on to outline additional key challenges to be aware of. She said most companies neglect to manage the customer service experience sufficiently and often lock the organisation into long-term outsourcing contracts without conducting appropriate pilot testing. She also pointed to risks related to knowledge management and retention, accentuated by the fact that customer service outsourcing providers have staff attrition rates of up to 70 to 80 percent, compared to an average of 19 to 25 percent in in-house contact centres.

Gartner concluded that there are benefits to be gained from outsourcing non-core processes, but rewards will not be instant and organisations should adopt a controlled and phased approach. Ms Bona advised organisations new to business process outsourcing to start by outsourcing onshore. „Don't be lured by the apparent cost appeal of placing end-to-end customer services processes in the cheapest offshore locations without conducting a thorough assessment of the transition methodologies of the off-shore provider, as well as your own ability to manage off-shore relationships."

Gartner recommendations for organisations when defining their customer service outsourcing strategy:

1. ***Identify objectives – be certain customer-facing business processes need to be outsourced.*** Businesses should only consider outsourcing non-core processes and those that are not key organisational competencies. Organisations should ask themselves two questions to identify if the process is core. Firstly, if we were building our business from scratch would we build this process or buy it? Secondly, are we so good at executing this process that other organisations might hire us to do it for them?
2. ***Map customer-facing processes from end to end and dedicate sufficient management resources to the intersection between outsourced and retained processes.*** A significant number of failures occur because organisations forget to map the entire customer process from the customer perspective. This frequently results in a poor customer service experience and sometimes customer defection. To be successful, organisations and outsourcers must understand the entire process and clearly articulate each party's entry and exit point.

3. ***Develop contracts that require innovation in service delivery to reduce the cost of ongoing operation.***
To avoid conflicts between the objectives of the enterprise and the goals of the outsourcer, customer service outsourcing contracts should not only be based on operational metrics such as number of calls handled or average call time. In this scenario, the outsourcer maximises profits by increasing the number of calls handled. Instead, contracts should include pricing related to service levels and customer satisfaction or other quality metrics to measure and motivate outsourcers.
4. ***Do not underestimate the management time required to make an outsourcing relationship work.***
Outsourcing should not be used as a means to offload the responsibility for problems. Effective integration of an outsourcer's services, to ensure it appears seamless to the customer is crucial. That integration needs careful and close management especially in the early stages of the relationship.

Eric Rey, Berne

Projektcontrolling

Projektcontrolling von Migrationsprojekten im Bereich der IT-Infrastruktur

1 IT-Infrastruktur – die Basis für alle geschäftskritischen Anwendungen

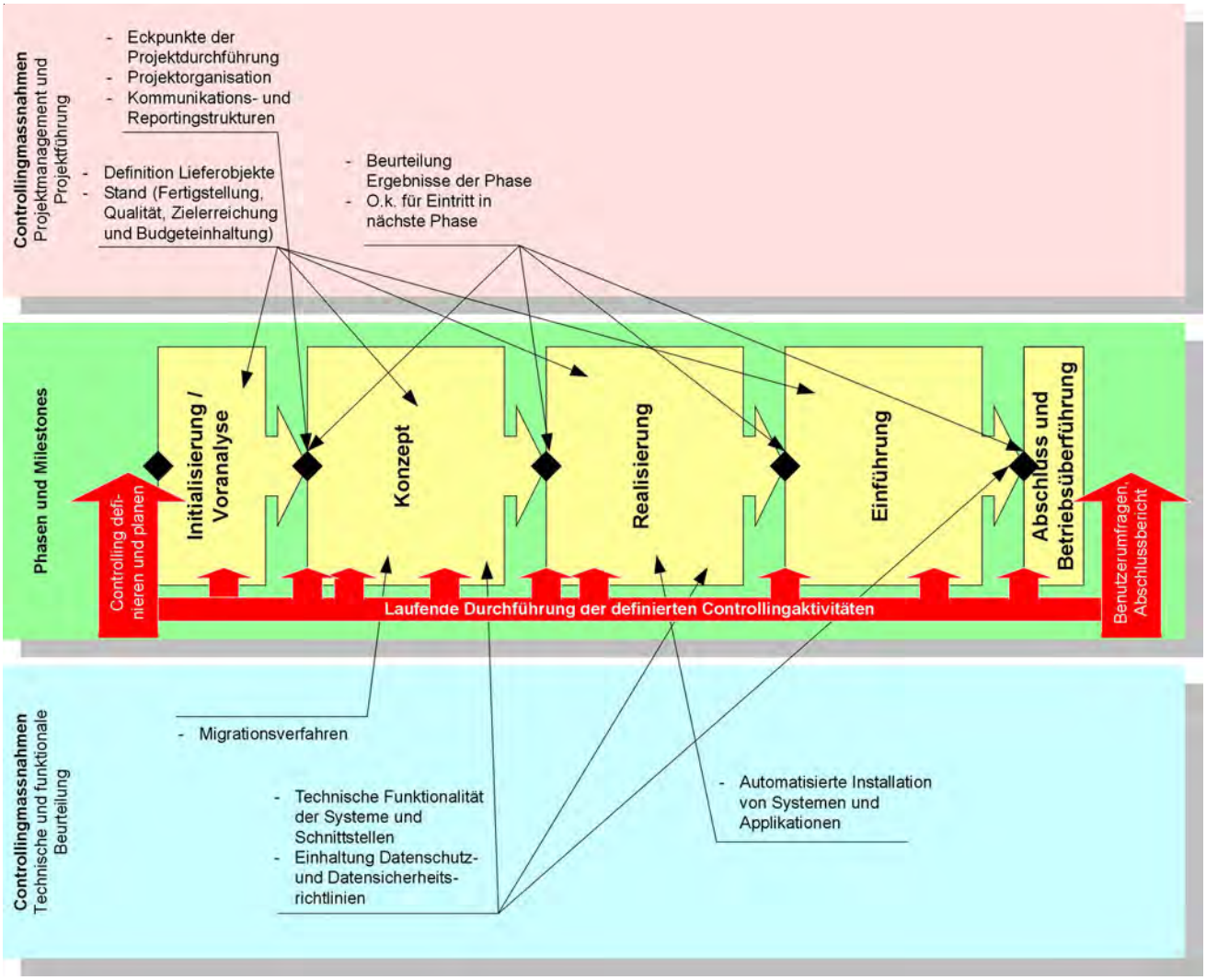
Die IT-Infrastruktur bildet die unverzichtbare Grundlage für die Bereitstellung der IT-Versorgung einer Unternehmung. Auf dieser IT-Grundversorgung basieren die business-relevanten Anwendungen. Jede Veränderung im Bereich der IT-Grundversorgung (IT-Basisinfrastruktur) hat direkte oder indirekte Auswirkungen auf die einzelnen Benutzer und deren Versorgung mit IT-Mitteln. Beispiele aus dem täglichen Leben illustrieren dies anschaulich. Am 7. Februar 2005 war zeitweise der gesamte SBB-Verkehrsknoten im Raum Zürich lahm gelegt. Durch Wartungsarbeiten an Systemen wurden Ausfälle dieser Systeme provoziert. Das Ergebnis war, dass während einigen Stunden auf bestimmten Streckenabschnitten kein Zug mehr fahren konnte, ja selbst der ganze Hauptbahnhof zeitweise praktisch ausser Betrieb gesetzt wurde.

Auch in weniger heiklen Umgebungen gilt es, je nach Grösse der einzelnen Projekte und deren möglichen Auswirkungen auf die betreffenden Geschäftsprozesse, geeignete Massnahmen zur Überprüfung des Projekterfolgs und der Zielerreichung zu ergreifen.

Es werden nachfolgend die folgenden Bereiche des Projektcontrollings unterschieden:

- Projektmanagement, Projektorganisation, Projektdurchführung
- Ergebnisse (funktionale, technische Zielerreichung, Qualität, Datenschutz und Datensicherheit)

Aus der Darstellung der einzelnen Punkte geht hervor, dass ein Controlling nicht allgemein definiert werden kann. Die hier dargelegten Punkte vermitteln einen Überblick über die relevanten Bereiche und über eine mögliche Durchführung. Nicht zuletzt hängt die Wirkung des Controlling davon ab, wie konsequent und gut es durchgeführt wurde und welche Massnahmen bei Abweichungen getroffen werden. Ein entscheidender Faktor in grossen IT-Infrastruktur-Migrationsprojekten besteht in der Erfahrung und im Leistungsausweis der betreffenden eingesetzten Projektmanager, sowie im Managementsupport seitens Auftraggeber (konsequente Umsetzung von Massnahmen, rasches und direktes Fällen von Entscheiden, Überwachung der Umsetzung von getroffenen Entscheiden und Durchsetzung derselben). Axept AG verfügt aufgrund von durchgeführten Grossprojekten bei national und international tätigen Kunden über eine umfangreiche Erfahrung im Projektmanagement und im Controlling des Projekterfolgs. Es sind hierbei insbesondere Vorhaben bei Kunden wie Helsana Versicherungen, Kantonale Verwaltung des Kantons Bern, XL Insurance Global Risk und SR Technics anzuführen.



2 Merkmale eines Migrationsprojekts

2.1 Umfang und Abgrenzungen von Infrastrukturprojekten

Die nachfolgend formulierten Betrachtungen gehen von der Realisierung von Migrationsprojekten aus, welche die folgenden Komponenten (je nach Situation auch nur Teile davon) tangieren:

- Serversysteme und dazugehörende Dienste, wie Verzeichnisdienste (z.B. AD, eDirectory, weitere), Kommunikationsdienste (DNS, DHCP) und Betriebssysteme
- Clientsysteme, Printing und deren automatisierte Verwaltung mit Softwareinstallation und -verteilung
- Systems Management Tools zur Überwachung der gesamten IT-Basisinfrastruktur
- Datensicherheit und Datenschutz und entsprechende Technologien (PKI, Secure-Mail, SingleSignOn, etc.)
- Netzwerkkomponenten (Firewall, LAN, WAN, MAN, etc.) und im Bereich des Netzwerks eingesetzte Technologien (WLAN, Internet, VPN, etc.)

Die Aufzählung ist nicht abschliessend. Sie umfasst die wesentlichen Bereiche von Infrastrukturprojekten. Je nach Anwendung und Situation können weitere Komponenten betroffen sein.

Im Umfang eines Migrationsprojekts werden bestimmte Technologien und /oder entsprechende Anwendungen (Betriebssysteme, Werkzeuge, Bürokommunikationsanwendungen) ersetzt, auf neuere Versionen migriert oder durch andere Systeme und Tools abgelöst.

2.2 Ausrichtungen und Zielsetzungen

Es kann festgehalten werden, dass heute praktisch keine Projekte in grösserem Umfang mehr realisiert werden,

- bei denen nicht ein unmittelbarer wirtschaftlicher Nutzen erwartet wird;
- deren Durchführung aufgrund von vorhandenen Abhängigkeiten (z.B. Kompatibilität von Anwendungen, auslaufender Support von Betriebssystemen) unumgänglich ist.

Im Wesentlichen gilt bei der Definition und während der Umsetzung der Grundsatz: IT for business! Somit muss während der gesamten Projektdurchführung weniger der technologische Ansatz im Vordergrund der Controllingmassnahmen stehen, sondern vielmehr der wirtschaftliche und funktionale Ansatz (welchen Nutzen bei welchem Aufwand erzielen wir für die Erbringung unserer Kernkompetenzen des Business damit?).

Oft wird in diesem Zusammenhang der Begriff „Bedürfniscontrolling" verwendet. Vorhaben werden vermehrt bezüglich des effektiv vorhandenen Bedürfnisses beurteilt. Nicht was technisch machbar ist, soll realisiert werden, sondern vielmehr das, was einen Mehrwert für die Erreichung der geschäftsrelevanten Zielsetzungen darstellt. Sehr oft werden auch grundsätzlich verschiedene Varianten präsentiert, die dann unter verschiedenen Kriterien (Wirtschaftlichkeit, Funktionalität, Abdeckung der Business-Bedürfnisse) beurteilt werden.

In jedem Fall (unabhängig von der Grösse des Projekts) liegt einer der wichtigsten Erfolgsfaktoren darin, die Projektdurchführung klar zu strukturieren. Als sehr wirksame Methodik erweist sich hierbei zum Beispiel Hermes2003, welche je nach Grösse des Projekts voll oder allenfalls sinngemäss anzuwenden ist.

3 Probleme und Checkpunkte

3.1 Bekannte Stolpersteine in IT-Infrastruktur-Migrationsprojekten

Aufgrund der Erfahrungen in grossen Projekten liegen die hauptsächlichen Stolpersteine in grösseren IT-Infrastruktur-Migrationsprojekten in folgenden Punkten begründet:

Bereich	Details	Massnahmen
Unklare Zielformulierung	Die Auftragssituation und die erwarteten Ergebnisse sind zu wenig klar definiert.	Von Beginn weg muss eine klare Formulierung der einzelnen Lieferobjekte erfolgen. Nebst den zu erarbeitenden Ergebnissen sind auch klare Abgrenzungen zu formulieren.
Veränderte Situationen und Anforderungen	Während dem Projektverlauf ändern oft die Umgebungsbedingungen. Neue Anforderungen entstehen, formulierte Rahmenbedingungen fallen weg bzw. werden geändert, technische Entwicklungen ermöglichen neue Lösungen.	Während dem Projekt muss laufend eine Beurteilung der funktionalen Anforderungen erfolgen. Allfällig veränderte Situationen müssen durch korrekt formulierte Changes beschrieben werden. Dem Projekt ist ggf. eine angepasste Ausrichtung zu geben.
Technische Probleme	Nach wie vor stellen technische Probleme bei der Projektdurchführung ein nicht zu unterschätzendes Risiko dar: ▪ Nicht nach Anforderung funktionierende Systeme und Applikationen rufen entsprechende Probleme hervor. ▪ Unvollständig oder nicht in wirklichkeitsnahen Umgebungen getestete Systeme und Applikationen geben ein falsches Bild der Funktionalität und führen zu Mehraufwendungen sowie zu unzufriedenen Benutzern. ▪ Probleme entstehen zudem bei der Datenmigration (nicht kompatible Softwareversionen) wie z.B. bei Dokumentenvorlagen, Access-Programmen, Makros in Dokumenten, etc.	Ein konsequentes phasenweises Vorgehen (z.B. nach Hermes2003) mit der Durchführung von entsprechenden Testprozeduren stellen sicher, dass Fehlfunktionen frühzeitig erkannt und ohne Einfluss auf die Benutzer durch entsprechend angepasste Lösungen abgefangen werden können. Der Einsatz einer geeigneten Test- und Integrationsumgebung ist je nach Projektgrösse ein absolutes Muss. Kontakte zu den Herstellerfirmen müssen durch geeignete Kanäle sichergestellt werden. Die involvierten Personen müssen über das notwendige produktspezifische Know-how verfügen (Einsatz von entsprechend zertifizierten Mitarbeitern).
Betriebsüberführung	Oft werden technisch sehr gute und funktionsfähige Lösungen entwickelt. Der Erfolg des Projekts kann aber trotzdem nicht erzielt werden, weil bereits während der Definition der Lösung ein ungenügender Einbezug des Betriebsteams erfolgte.	Frühzeitiger Einbezug der Betriebscrew. Adäquater Mitentscheid der Betriebs-Mitarbeiter bei der Definition der Lösungen, Lösungsvarianten und der eingesetzten Produkte.

Praxisbeispiel: In einem Migrationsprojekt kommt eine Vielzahl von Wordvorlagen zum Vorschein, welche bei der Ist-Aufnahme nicht erfasst wurden. Diese enthalten jedoch Makros, die jeweils einzeln angepasst werden müssen, da sie nicht mehr mit der neuen Office-Version kompatibel sind.

3.2 Projektcontrolling in zwei Bereichen

Die nachfolgend aufgeführten Punkte sind nicht als „abschliessende Projektcontrollingmassnahmen“ zu betrachten. Nach Hermes2003 sind entsprechende QS-Pläne zu erstellen, welche allgemein die QS innerhalb des Projekts sicherstellen. Nachfolgend sind einige wichtige Punkte als „best practice“ dargestellt, welche oft bei reinen QS-Massnahmen eher zu kurz kommen, jedoch bezüglich des Projektfortschritts und der Beurteilung der Qualität der erarbeiteten Resultate wichtige Hinweise geben.

3.2.1 Bereich Projektmanagement und Projektdurchführung

Prüfpunkte	Prüfkriterien	Prüfzeitpunkt
Eckpunkte der Projektdurchführung	▪ Projektauftrag, Zielsetzungen, und erwartete Resultate ▪ Realistische Termin- und Vorgehensplanung ▪ Mittelbedarf über das gesamte Vorhaben, Wirtschaftlichkeit ▪ Konsequenzen bei Realisierung und bei Nicht-Realisierung	Projektinitialisierung
Projektorganisation	▪ Zweckmässigkeit der Projektorganisation (sinnvolle Grösse, kein „oversizing“ durch möglichst viele Gremien) ▪ Auftraggeber ist klar ▪ Umsetzungsteams sind definiert ▪ Sinnvoller Einbezug des IT-Betriebs geht aus der Projektorganisation hervor	Projektinitialisierung
Kommunikations- und Reportingstrukturen	▪ Reporting über Projektstand an die betreffenden Gremien (Projektleitung, Auftraggeber, ev. Steeringboard) ▪ Kommunikation, Information, Projektmarketing an die Betroffenen	Projektinitialisierung
Ergebnisse der einzelnen Phasen und damit Freigabe der nächsten Phase	▪ Z.B. gemäss den Formulierungen nach Hermes2003 ▪ Laufendes Bedürfniscontrolling (entsprechen die Ergebnisse und Zielsetzungen nach wie vor den vorhandenen Bedürfnissen?)	Bei Phasenabschluss vor Eintritt in die nächste Phase
Definition der Lieferobjekte	▪ Abnahmekriterien der einzelnen Lieferobjekte ▪ Verantwortlichkeiten der Lieferobjekte ▪ Termine (z.B. bei technischen Konzepten: bereit für Review, bereit für Abnahme, Hinweis auf Abnahmedokumente)	Projektinitialisierung Laufend während gesamtem Projekt
Termine, Qualität, Budget	▪ Konkrete Überprüfung der Termineinhaltung der Fertigstellung der einzelnen Lieferobjekte, der Qualität derselben und des Einsatzes der finanziellen Mittel unter Bezug auf den Fertigstellungsgrad. ▪ Treffen von Massnahmen bei Abweichungen (formulieren von Changes, Reduktion der geforderten Funktionalität, etc.)	Laufend während gesamtem Projekt

3.2.2 Technische und funktionale Beurteilung der Ergebnisse

Prüfpunkte	Prüfkriterien	Prüfzeitpunkt
Technische Funktionalität der Systeme und der Schnittstellen	▪ Kompatibilität mit anderen Systemen (z.B. Betriebssysteme/Datenbanken mit Anwendungen) ▪ Beurteilung Abdeckung der Bedürfnisse und Anforderungen der Benutzer/der Unternehmung durch die Lösung (funktional, technisch, organisatorisch, betrieblich) ▪ Verfügbarkeit von Test- und Integrationssystemen sowie der zugehörigen Prozesse und Prüfverfahren ▪ Einhaltung der Test- und Integrationsprozesse sowie der Prüfverfahren ▪ Vorliegen von Prüf- und Abnahmeprotokollen	Beurteilung Ende Phase Konzept Gesamtfunktionalität überprüfen Ende Phase Realisierung Test und Abnahme Gesamtsystem nach erfolgter Einführung
Datenschutz und Datensicherheit	▪ Geeignete Schutzmassnahmen im Bereich Virenschutz, automatisiertes Patch-Management ▪ Datenzugriff (Administrations- und Rollenkonzepte, Berechtigungskonzepte) ▪ Abrufverfahren von Personendaten (Definition, welche Daten in den Systemen gespeichert und abrufbar sind) und Überprüfung Einhaltung der geltenden Vorgaben und Richtlinien	Bei Phasenabschluss Konzept Nach erfolgter Einführung bei Gesamtabnahme
Migrationsverfahren	▪ Technisches Migrationsverfahren (Datenmigration, Benutzer und Berechtigungen, Portierung z.B. Mailboxen, Dokumentenvorlagen/Makros, etc.) ▪ Organisatorische Bereiche der Migration (Unterbrüche, Kommunikation an Betroffene, Ausbildung und Einführung der Benutzer) ▪ Wiederherstellung des ursprünglichen Zustandes sollte jederzeit möglich sein bzw. beim Überschreiten des „point of no return“ sind vorgängig entsprechende Risikobetrachtungen inkl. Definition von Massnahmen bei Eintritt des Risikos anzustellen	Ergebnisse sollen nach Abschluss der Phase Konzept vorliegen
Automatisierte Installation von Systemen und Applikationen	▪ Definierte Prozesse für Applikationspaketierung mit klarer Rollenbeschreibung (inkl. Einbezug des Applikationsfachverantwortlichen) ▪ Umfassende Tests in der produktionsnahen Umgebung (realitätsnahe Tests) ▪ Definition und Durchführung von systemtechnischen (Verträglichkeit in Gesamtumgebung) und fachtechnischen Tests (Funktionalität der betreffenden Anwendungen) ▪ Definition von Wiederherstellungsprozeduren (Backup/Restore, Desaster Recovery) inkl. der betreffenden System- und Prozessdokumentationen	Je Applikationspaket bzw. automatisiert installiertes System (Server, PC, Drucker)

Praxisbeispiel: Die Applikationspaketierung wurde zwar gemäss einem definierten Prozess in mehreren Stufen (Paketierung, Systemtest, Benutzertest) durchgeführt. Das Problem bestand aber darin, dass die Testumgebung nicht ein wirkliches und umfassendes Abbild der produktiven Umgebung darstellte. Trotz „erfolgreich“ durchgeführten Tests, entstanden technische und funktionale Probleme bei der Ausbreitung und im täglichen Gebrauch der einzelnen Applikationspakete.

3.3 Durchführung der Überprüfungs- und Controllingmassnahmen

Aktivität	Details
Planung der betreffenden Controllingmassnahmen und konsequente Durchführung	Ein „Projekctontroller“ hat seine Massnahmen nach folgenden Gesichtspunkten zu planen: ▪ Welche Aussage bezüglich der durchgeführten Controllingmassnahmen will ich machen? ▪ An wen rapportiere ich die Ergebnisse? ▪ Wann führe ich welche Controllingaktivität durch? ▪ Wie informiere ich die Betroffenen der Projektteams? ▪ Welche Eskalationsstufen bestehen und wie können Massnahmen eingeleitet und umgesetzt werden?
Regelmässiges standardisiertes Reporting zuhanden des Auftraggebers und ev. Steeringboard	Ein aussagekräftiges Reporting, welches als effizientes Steuerinstrument eingesetzt werden kann, soll folgende Inhalte aufweisen: ▪ Gesamtbeurteilung ▪ Zielerreichung ▪ Termine ▪ Budget ▪ Personal / Teams ▪ Qualität
Stichprobenweise Überprüfung nach Checklisten gemäss individuellem Projektfortschritt	Gemäss den unter Kapitel 3.2 aufgeführten Checkpunkten werden entsprechende Checklisten zusammengestellt. Die Überprüfungsmassnahmen werden durchgeführt und die Ergebnisse werden mit Formulierung von Empfehlungen und durchzuführenden Massnahmen (ev. Stellungsnahmen) an die entsprechenden Stellen (Projektleitung und direkte Verantwortliche, Finanzkommissionen, Auftraggeber, Management, etc.) abgegeben.
Umfragen bei den Benutzern – Auswertung von Calls des Helpdesks	Aus sinnvoll durchgeführten Umfragen bei den Benutzern (z.B. nach erfolgter Einführung oder nach Durchführung einer Ausbildung) können wertvolle Schlüsse für zukünftige Vorhaben gezogen werden. Solche Umfragen sind aber möglichst einfach und praktisch handhabbar zu gestalten (Einsatz von webbasierenden Services, werden z.B. als Service am Markt angeboten und müssen nicht selbst entwickelt werden).

Simon Roggli, Consultant Axept AG, Schönbühl-Bern

Audit Software

Datenprüfung im Werkzeugkasten der Revision

Datenprüfungswerkzeuge gehören in den Werkzeugkasten des Revisors, wie früher der Bleistift und die Rechenmaschine. In einem komplexen Systemumfeld, wie z.B. SAP, sind klassische manuelle Ansätze von vornherein zum Scheitern verurteilt. Dokumentiert wird diese Entwicklung nicht zuletzt durch den Einsatz von WinIdea, einem der verbreitetsten DP- Werkzeuge, durch die Betriebsprüfung im Rahmen der steuerlichen Außenprüfung. Wie der folgende Artikel zeigt, ist mit dem Einsatz eines Werkzeuges die Palette der Möglichkeiten aber bei weitem noch nicht erschöpft.

1. Was ist Datenprüfung?

Bevor man sich mit den Werkzeugen der Datenprüfung und ihrem Einsatz auseinandersetzt, muss im ersten Schritt geklärt werden, was unter Datenprüfung zu verstehen ist.

„Datenprüfung ist eine Verfahrensweise bzw. Prüfungstechnik für die Auswertung von Unternehmensdaten zur Unterstützung bzw. Durchführung von Prüfungshandlungen in sämtlichen Prüfungsmethoden mit Systemprogrammen auf der Unternehmens-EDV oder mit prüfereigenen Programmen auf dem Prüfer-PC .“

2. Werkzeuge der Datenprüfung

Zur Unterstützung bei der Analyse und Auswertung von Massendatenbeständen, z.B. bei Migrationen, logischen Verknüpfungen, Aufbereitung der Daten etc., kann sich der Revisor verschiedener Datenprüfungswerkzeuge bedienen.

2.1 Office-Programme

Weit verbreitet, da auf fast jedem Revisoren-PC vorhanden, sind Tabellenkalkulations- und Datenbanksysteme, wie z.B. Excel oder Access von Microsoft. Die Vorteile dieser Produkte liegen in der Verfügbarkeit der Standardsoftware, ihrer vermeintlich einfachen Handhabung und dass es sich in der Regel um ausgereifte Anwendungen handelt. Die schwerwiegenden Nachteile dieser Werkzeuge der individuellen Datenverarbeitung sind vor allem

- Schwierigkeiten mit großen Datenmengen
- erhöhte Fehlerrisiken
- fehlende Revisionssicherheit

2.2 Drucklistenanalyse

Für die berichtsbezogene Datenuntersuchung (Datenprüfung auf Basis von Drucklisten/Reports), Datenanalyse und Datenumwandlung existieren spezielle Softwareprodukte wie z.B. Monarch oder DataImport, die es dem Prüfer ermöglichen, ohne Programmierkenntnisse komplexe Druckdateien auszuwerten. Bei diesen Programmen sind die Analysefunktionen in der Regel nur schwach ausgeprägt.

2.3 Professionelle Datenprüfungssoftware (ACL und IDEA)

Als Revisionswerkzeuge zur professionellen Datenprüfung von umfangreichen Datenbeständen und/oder Reports werden ACL (Audit Command Language) und IDEA (Interaktive Datenextraktion und -analyse) angeboten.

Es handelt sich um Softwaretools mit revisionsspezifischen, definierten Selektier- und Analysefunktionen, umfangreichen Schnittstellenfunktionalitäten und Sprachelementen für diverse Operationen zur individuellen Programmierung. Die Software ist auf unterschiedlichen Systemplattformen lauffähig und revisionssicher, d.h. sie verfügt über eine Verarbeitungshistorie, und die Originaldaten sind nicht veränderbar.

Die Datenprüfungswerkzeuge bieten diverse formale, logische, mathematische und statistische Operationen sowie analytische Prüfungshandlungen auf der vom Unternehmenssystem auf das Prüfersystem übertragenen Datenbasis. Die Funktionen dieser Programme ermöglichen zum Beispiel die Ermittlung von absoluten oder ganzzahligen Werten, eine Altersbestimmung oder einen Datumsvergleich sowie die Konvertierung eines numerischen Ausdruckes in eine Zeichenfolge und umgekehrt – hilfreiche Funktionen beim Vergleich von Daten.

Die Möglichkeiten der Prüfungshandlungen sind vielfältig:

1. Sortierung, Klassifizierung und/oder Verdichtung eines Datenbestandes nach jedem denkbaren Merkmal, z.B. Bewertungsklassen oder Filialen.
2. Zusammenführung und Vorher-/Nachher-Vergleich von zwei Dateien, z.B. um eine Migration oder EURO-Umstellung zu prüfen.
3. Differenzen- und Verhältnisbildung zur Bewertung einer Abstimmhandlung und/oder Bestimmung einer Einzelfallprüfung.
4. Formal- und Plausibilitätsprüfung auf bestimmte Datenfeldinhalte, z.B. ob ein logischer Wert im Feld „Alter“

steht oder ob ein Schadeneintrittsdatum nach dem Meldedatum liegt.
5. Oder die Schaffung eines einfachen Überblicks über das Datenvolumen und die Wertigkeit von z.B. Debitoren-OPs oder des Materialbestands.

Die langjährige praktische Anwendung der inhaltlichen Datenprüfung hat gezeigt, dass sie ein wichtiges Werkzeug der IT-Revision darstellt. Gute Kenntnisse über die zu prüfenden Anwendungen und Daten inklusive einer sorgfältigen Planung der Datenprüfung sind allerdings unerlässlich. Gewissenhaftes Arbeiten, eine vollständige Ergebnisdokumentation sowie die Interpretation der Prüfungsergebnisse führen zu repräsentativen Prüfungsfeststellungen, die mit den gewohnten Prüfungstechniken nicht oder nur mit hohem Zeitaufwand zu leisten sind.

3. Datenprüfung von SAP

Bei SAP R/3 handelt es sich um eine weit verbreitete Standardsoftware. Das bedeutet, insbesondere für die externen Revisoren, dass sie früher oder später mit einem SAP-System konfrontiert werden. Der Revisor hat es hier mit einer komplexen und sich ständig ändernden Systemlandschaft zu tun (ein SAP-Releasewechsel kann prüferisch schlimmer sein als eine komplette Systemmigration!), so dass der Revisor sich ständig an veränderte Funktionalitäten und Tools anpassen muss. Dazu kommen ein komplexes Datenmodell und ein diffiziles Berechtigungskonzept, was häufig zu einer vereinfachten Berechtigungsvergabe führt, was im schlechtesten Fall „Administratorrechte (SAP_ALL) für alle“ bedeutet..

Zur Bewältigung und Unterstützung von komplexen SAP R/3-Prüfungen sind softwaretechnische Hilfsmittel sinnvoll.

3.1 SAP AIS

Das SAP R/3 Audit Information System, kurz AIS genannt, wurde von der SAP AG als Prüfungstool zur Unterstützung von Wirtschaftsprüfern, internen Revisoren, Systemprüfern und Datenschutzbeauftragten unter Berücksichtigung von Anforderungen durch den SAP-Arbeitskreis Revision entwickelt.

Das AIS ist kein Datenprüfungswerkzeug im klassischen Sinne, sondern der Datenprüfung vorgelagert.

Das AIS ist eine überwiegend an den Prüfungsanforderungen und -standards der internen und externen Revision orientierte Systemkomponente zur Durchführung von Kontroll- und Prüfungsaufgaben online am SAP R/3-System.

Die verfügbaren Daten und Auswertungen – genutzt werden SAP Standardprogramme und Funktionen - sind zwei Hauptgruppen zugeordnet:
1. System Audit
2. Kaufmännisches Audit

Die Sichtweise des „System Audit“ bezieht sich im wesentlichen auf die SAP R/3-Systemkonfiguration und richtet sich verstärkt an den IT-Revisor, Systemadministrator und Datenschutzbeauftragten.

Das „Kaufmännische Audit“ ist für Mitarbeiter der Wirtschaftsprüfungsgesellschaften und des Controllings im Unternehmen von größerem Interesse, da es das Hauptbuch als zentrale Komponente des betrieblichen Rechnungswesens abbildet.

Die bessere Übersicht der zur Verfügung stehenden Informationen verkürzt die Prüfungszeit, d. h. die Prüfung wird durch AIS unterstützt und vereinfacht.

Es stellt Schnittstellen zum Download von Rohdaten, Saldenlisten und Bilanzen für die Verarbeitung mit Fremdsystemen, z.B. AuditAgent oder ACL/IDEA zur Verfügung.

Dem Revisor bieten sich durch das AIS folgende Vorteile:
1. Die Benutzeroberfläche lässt sich auf die individuellen Anforderungen der Benutzer einstellen.
2. Im kaufmännischen und systemtechnischen Bereich werden umfangreiche Auswertungsmöglichkeiten geboten.
3. Daten werden komfortabel und übersichtlich bereitgestellt.
4. Der Prüfer ist unabhängig von Dritten, d.h. er gibt den Anstoß zur Ermittlung von Arbeitsergebnissen und nicht der Unternehmensmitarbeiter.
5. Die zur Verfügung stehende Datenbasis steht für einen hohen Detaillierungsgrad, verbunden mit guter Selektier- und Strukturierbarkeit.
6. Die Daten lassen sich zeitnah und mit geringem Aufwand gewinnen.
7. Die direkte Erhebung von Daten auf System- und Datenbankebene gewährleistet einen hohen Grad an Aktualität, Objektivität und Unverfälschtheit der Daten.

Auch der ungeübte SAP-Prüfer kann sich über das AIS schnellen Zugriff auf die gewünschten Informationen verschaffen, wobei die Stärken des AIS im Allgemeinen in der aktuellen Datenbasis und im Speziellen im System Audit liegen.

Nachteilig wirkt sich, zumindest für die externe Revision, die örtlich begrenzte Nutzung am SAP-System aus. Das AIS ist als prüfungsunterstützendes Tool konzipiert, d.h. es kann nicht generell Prüfungsansätze und -programme abbilden und entbindet den Revisor nicht von der sorgfältigen Festlegung der Einzelziele der Prüfung und der dazu erforderlichen Datenbasis im vorhinein.

3.2 CheckAud for SAP R/3 Systems

CheckAud for SAP R/3 Systems, kurz CheckAud genannt, von der ibs schreiber gmbh entwickelt und von SAP zertifiziert, hat als maßgebliche Zielrichtung das Berechtigungskonzept transparent und leicht auswertbar sowie die sicherheitsrelevanten Bereiche eines SAP R/3-Systems prüfbar zu machen.

Das Programm ist in zwei Module aufgeteilt, die es dem Revisor ermöglichen, die Aufnahme des SAP-Systems vor Ort mit dem Scan-Modul durchzuführen und die Prüfung mit dem Auswertmodul an der eigenen Arbeitsstation auszuführen.

In den Leistungen von CheckAud spiegeln sich gleichzeitig die Verarbeitungsschritte wieder, wie eine Untersuchung des SAP-Systems mit CheckAud effizient durchgeführt werden kann:

1. Das SAP-System wird vom Prüfer (minimale Zugriffsberechtigungen erforderlich) selbst oder einem Administrator gescannt.
2. Systeminformationen stehen zur Verfügung, z.B. welches Betriebssystem, welches Release und welche Datenbank eingesetzt wird.
3. Die automatische Analyse der Aufnahme zeigt dem Prüfer eine umfangreiche Auswertung über allgemeine Benutzerinformationen, wie abgelaufene, gesperrte oder ungenutzte Benutzerkonten.
4. Automatische Analyse der Systemparameter und Vergleich mit eigenen Vorgabewerten.
5. Die Standardberichte mit detaillierten Informationen zu den jeweils ausgewählten Objekten werden halbautomatisch aus der Aufnahme gepflegt.
6. Auswertung der R/3-Tabellen nach Änderungskriterien und Berechtigungen.
7. Darstellung der Organisationsstruktur für die Prüfung der Zugriffsberechtigungen in Baumstruktur, um gegebenenfalls Besonderheiten zu erkennen.
8. Die Abhängigkeiten des Berechtigungskonzeptes (welchen Benutzern wurde z.B. das Profil SAP_ALL zugeordnet) können in drei unterschiedlichen Baumstrukturen dargestellt werden.
9. Die Zugriffsberechtigungen des SAP-Systems können interaktiv ausgewertet werden, z.B. eine Liste aller Benutzer anzeigen, die beliebige oder ausgewählte Rechte haben.
10. Eine komfortable Möglichkeit ist die Prüfung der Zugriffsberechtigungen über die Transaktionen; Transaktions- und Anwendungsberechtigungen ausgewertet werden können.
11. Über CheckAud können kritische Berechtigungen und Kombinationen aus beliebig vielen Berechtigungsobjekten definiert und automatisch geprüft werden.
12. Es können Systemaufnahmen (z.B. Vorjahr und Prüfungsjahr) miteinander verglichen und analysiert werden.

Mit CheckAud bietet sich dem Revisor eine komfortable Möglichkeit, die Zugriffsberechtigungen eines SAP R/3-Systems in einem angemessenen Zeitrahmen außerhalb des SAP-Systems zu prüfen.

Die Auswertung der betriebswirtschaftlichen Daten wird nicht unterstützt.

3.3 SQUARE

SQUARE (SAP Quick Audit Review oder auch SAP-Schnelltest) ist eine Sammlung von Datenprüfungsskripten und Masken auf Basis von ACL.

Auch für die Analyse von Daten des SAP-Systems gilt das Pareto-Prinzip. Mit 20 % des Aufwandes lassen sich 80 % des Ergebnisses erzielen. Der SAP-Schnelltest SQUARE ist nach diesem Prinzip konzipiert. Der SAP-Schnelltest erhebt nicht den Anspruch, wesentliche Geschäftsprozesse in größter Tiefe prüferisch zu durchdringen. Der SAP-Schnelltest soll durch wenige Analyseschritte Risikoindikatoren beleuchten, erste Anhaltspunkte für spätere Prüfungsfeststellungen liefern und „intelligente“ Stichproben auswählen, die eine weitere Einzelfallprüfung erlauben.

Der SAP-Schnelltest untersucht Bestands- und Bewegungsdaten aus den Bereichen

- SAP Basis und Benutzerverwaltung
- Hauptbuchhaltung
- Kreditorenbuchhaltung
- Debitorenbuchhaltung
- Anlagenbuchhaltung
- Materialwirtschaft

Für die Jahresabschlussprüfung ist der SAP-Schnelltest im Bereich der Prüfungsplanung einzuordnen. Anhand der Ergebnisse lassen sich Schlussfolgerungen über die Wirksamkeit des internen Kontrollsystems im Rahmen des SAP-Systems und weitere risikoorientierte Detailprüfungsschritte ableiten.

Für den Revisor außerhalb des Jahresabschlusses liefert der SAP-Schnelltest Informationen über mögliche Manipulationen am System, über signifikante Eingabe- oder Verarbeitungsfehler (Fraud & Error) und grundsätzliche Unstimmigkeiten. Eine Interpretation von verdächtigen Einzelfällen erfolgt im Rahmen von SQUARE nicht.

4. Prüfung der individuellen Datenverarbeitung

In den Fachabteilungen der Unternehmen wird verstärkt mit individueller Datenverarbeitung (kurz IDV genannt) gearbeitet. Im Wesentlichen betrifft dies den Einsatz von Microsoft Excel. Damit ist auch die Prüfung von Excel-

Dateien ein Bestandteil eines ganzheitlichen Datenprüfungsansatzes.

Excel-Dateien sind nicht unproblematisch, da Auswertungen per End-Anwendertools generell über ein hohes Fehlerpotential verfügen.

Die Probleme bei der Entwicklung von Auswertungen Excel durch Endanwender stellen sich wie folgt dar:
1. Die Endanwender verfügen in der Regel nur über autodidaktische Fähigkeiten im Umgang mit Excel, d.h. nicht ausreichend geschultes Personal nimmt Aufgaben der EDV-Abteilung/ Programmierung wahr.
2. Dazu kommt eine „unkontrollierte" Entwicklung der Anwendung, mangels konkreter, im Projektteam erarbeiteter Vorgaben und Pflichtenhefte, und vorbei an jeglichen Programmierstandards.
3. Es werden keine geregelten Abnahmeverfahren und Tests durchgeführt. Der Entwickler kontrolliert sich selber und testet seine Auswertungen selber.
4. Der Anwender ist zugleich Herr über die Anwendungen und Daten, was zu einer unkontrollierten Nutzung der Programme führen kann. Es fehlen häufig Restriktionen für den Einsatz und die Weiterverarbeitung der Daten und Anwendungen, z.B. nach dem 4-Augen-Prinzip.

Daraus resultiert ein hohes Risiko, doch umfangreiche Excel-Sheets sind manuell fast unmöglich zu prüfen.

Die hohe Fehleranfälligkeit und schwere Prüfbarkeit macht Excel-Auswertungen leicht manipulierbar. Die kleinste Veränderung eines Faktors in einer komplexen, scheinbar gleichlautenden, Formelreihe in ein oder zwei Zellen kann ein Ergebnis maßgeblich verändern.

Warum sind Excel-Auswertungen so fehleranfällig ?
1. Häufig basieren falsche Ergebnisse auf Formelfehlern. In den seltensten Fällen handelt es sich bei den Anwendern um EDV-Spezialisten. Daraus resultiert das Risiko technisch falsch angewandter Formeln. Durch Unachtsamkeit beim Markieren kommt es zu Bezugs-Fehlern. Wurde evtl. eine Zelle zuviel oder wurden im umgekehrten Fall nicht alle benötigten Zellen markiert, ist der Fehler vorprogrammiert.
2. Üblich sind in Excel-Dateien Verweise auf andere Excel-Anwendungen, um mit deren Inhalt zu arbeiten. Ändert sich zwischen zwei Verarbeitungen durch Verschieben oder Löschen der Pfad der Datei, kann Excel die entsprechenden Daten nicht finden.
3. Ohne Sicherheitsabfragen passiert es häufig, dass Zelleninhalte ungewollt überschrieben oder gelöscht werden.
4. Über die vorgenommenen Veränderungen der Tabelle existiert kein Nachweis, es wird keine Verarbeitungshistorie geführt.
5. An IDV-Anwendungen werden häufig nicht die gleichen Dokumentationsanforderungen gestellt wie für Standardanwendungen üblich, wodurch die Prüfbarkeit und Nachvollziehbarkeit der Anwendungen erschwert oder unmöglich wird.
6. Durch die fehlende Dokumentation entsteht möglicherweise eine Abhängigkeit zum Entwickler der Auswertungen. Das Herrschaftswissen bezüglich der Basisdaten und ihrer zum Teil sehr komplexe Weiterverarbeitung macht die Pflege durch Dritte schwierig, wenn nicht sogar unmöglich.

Mit Softwaretools, wie z.B. SpACE (steht für Spreadsheet Auditing from Customs and Excise), existieren Werkzeuge für die Prüfung von Excel-Dateien. Damit lassen sich selbst in äußerst komplexen Spreadsheets Fehler und Manipulation aufdecken.

Die Erfahrung zeigt, dass ca. 10 % aller Excel-Dateien signifikante Fehler enthalten, Hochschulforschungen sprechen z.T. sogar von einer Fehlerrate zwischen 25 und 80 Prozent.

Bei SpACE handelt es sich um ein relativ einfach anzuwendendes Tool, das als „add in" in der gewohnten Excel-Umgebung angewendet wird.

Die Darstellung der Ergebnisse ist so simpel wie wirkungsvoll. Das Prinzip der Analyse basiert auf einer Farbcodierung der enthaltenen Muster. Unterschiedliche Inhalte in Zellen, z.B. numerische Werte oder Text sowie abweichende Formeln, werden andersfarbig dargestellt. D.h., es ist auf den ersten Blick zu erkennen, wenn ein Muster durchbrochen wurde und sich Ansatzpunkte für genauere Prüfungshandlungen ergeben.

Formelstrukturen werden verglichen, unterschiedlich aufgebaute Formeln werden in abweichenden Farben codiert und die Häufigkeit der verwendeten Formel ist erkennbar. Bestehende Abhängigkeiten zwischen den Formeln sowie zu anderen Arbeitsblättern und Excel-Dateien werden aufgezeigt. Enthält ein Arbeitsblatt versteckte Zeilen oder Spalten, werden diese in den Analyseblättern dargestellt und farblich markiert. Zellen mit unterschiedlichen Formatierungen sind durch die andersfarbige Darstellung in SpACE eindeutig identifizierbar.

Weitere Funktionen sind z.B.:
- Informationen über die komplette Excel-Datei mit allen angesprochenen Links zu anderen Dateien,
- eine Grobanalyse über das Arbeitsblatt mit Art und Anzahl der Zellen,
- Informationen über WERTE in abgelegenen Zellen, die vielleicht außerhalb des Sichtbereichs liegen.

Fehlende Plausibilitätsprüfungen bei den Excel-Auswertungen bergen das hohe Risiko, dass Fehler nicht erkannt

und Unternehmensentscheidungen maßgeblich fälschlicherweise beeinflusst werden.

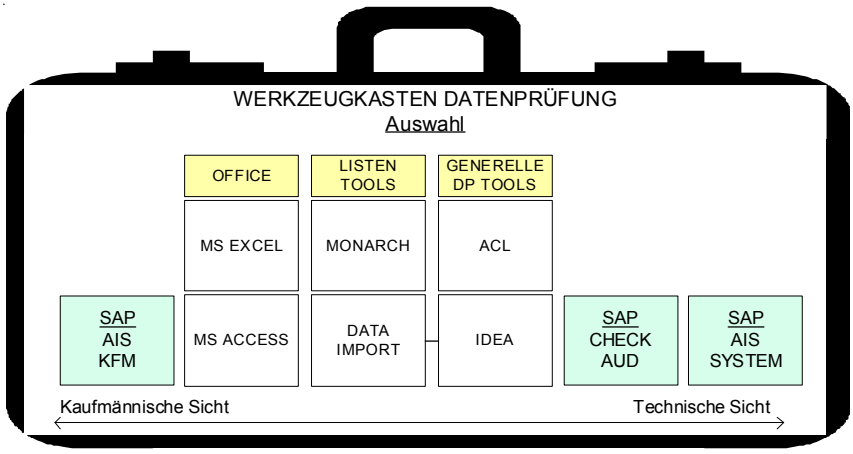
Jedes noch so gute interne Kontrollsystem, ebenso wie perfekte revisorische Prüfungshandlungen, werden durch eine unsachgemäße und ungeprüfte Weiterverarbeitung der Daten mit Excel unterwandert.

5. Fazit

Die Bandbreite und Nutzungsmöglichkeiten von Datenprüfungswerkzeugen ist größer als üblicherweise bekannt. Es ist in jedem Fall sinnvoll, sich intensiv vor dem Einsatz der genannten Werkzeuge mit ihrem Nutzen für die Prüfung auseinanderzusetzen. Dies gilt natürlich besonders vor dem Hintergrund, dass, obwohl Lizenzen in der Regel teuer sind, der wesentliche Kostenanteil in der Einarbeitungs- und notwendigen Arbeitszeit liegt.

Trotzdem ist eine effektive Prüfung ohne den Einsatz von Softwarewerkzeugen kaum möglich.

Claudia Stange, Grant Thornton Deutschland GmbH



Express Line

A Word from the Chair

Greetings!

A new presentation with audio is available to demonstrate the many benefits of ISACA® membership. The presentation can be accessed online at www.isaca.org/memberorientation.

The annual purge of members will take place 1 April. After this date, members who have not renewed will no longer have member access to the ISACA web site and will not receive any further issues of the ***Information Systems Control Journal®***. Until the purge occurs, members can renew online at www.isaca.org.

Sunil Bakshi

2003 CISA® Audit

The audit of documentation for 2003 continuing professional education (CPE) activities began recently. A randomly selected group of those holding the Certified Information Systems Auditor™ (CISA) designation has been sent an audit letter requesting written support documentation for 2003 CPE hours. Please direct member questions about the 2003 audit to the certification department at certification@isaca.org or +1.847.253.1545, ext. 471, 403 or 474.

CISA Job Analysis

The CISA job analysis project was recently completed and the results reported to ISACA's CISA Certification Board. The results will help ensure that the CISA exam continues to meet the highest standards for professional certification and is representative of the work and knowledge required of CISA holders in practice. The results will be posted to the ISACA web site in June 2005 and will serve as the basis for the 2006 CISA exam.

ISACA offers many thanks to the CISA holders who participated in the project.

New CISM Job Practice Analysis Begins

ISACA has begun a CISM job practice analysis study to update the criteria used to certify and examine CISM candidates. The current job practice analysis is international in scope and supported by other security management organizations, including the Information Systems Security Association, the Information Security Forum and ASIS International. Each of these organizations has contributed a member to the task force. As part of this process, a series of task force meetings and focus panels has been scheduled to gather information from experienced practitioners. The initial task force meetings began in early 2005, and work should be complete by the end of the year. Results will be implemented in future exams.

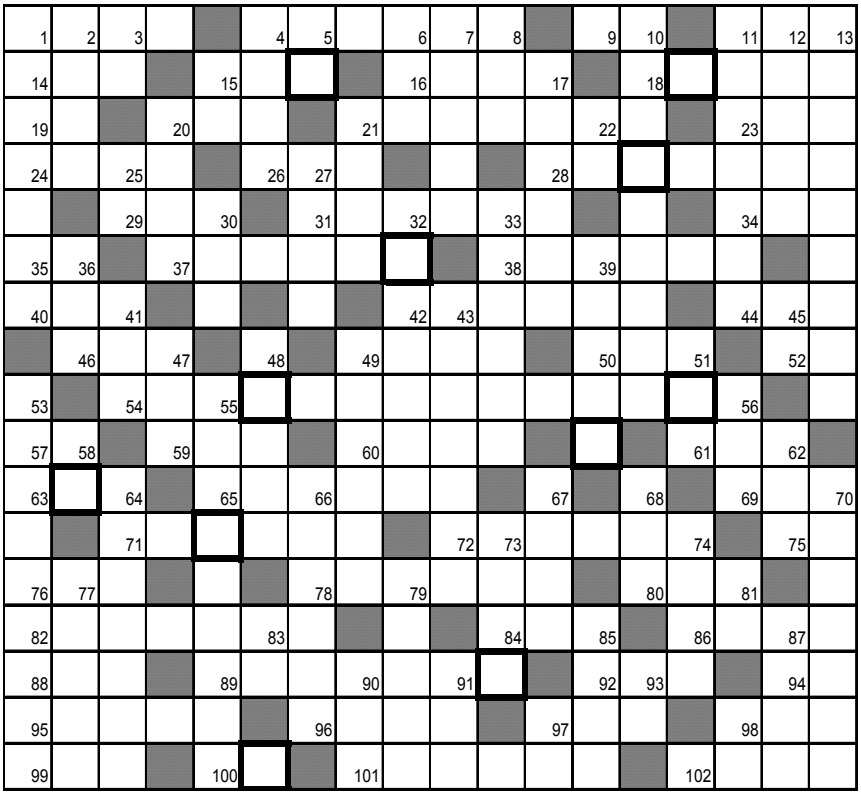
To participate in focus panels or recommend subject matter experts for future reviews, please contact Ron Hale at rhale@isaca.org or +1.847.590.7492. %

Online Career Center

ISACA will unveil an online career center for organizations seeking to hire and IT professionals searching for a job. ISACA members will have the added advantage of being eligible to receive e-mail notification when new job opportunities are posted. Please visit www.isaca.org/jobs for the latest details on this new offering.

The ISACA Crossword Puzzle 2/05

Dieses Rätsel ist auf deutsch und hat mit dem Schwerpunktthema dieser Nummer zu tun. Autor ist der Redaktor. Lösungen, Kommentare und Reklamationen sind an ihn zu richten.



Waagrecht: 1 ***Messgrösse für magnetische Datenträger***; 4 Form von ***locken;*** 9 ***Gegenstand der Untersuchungen***; 11 „tiefe“ Vorsilbe; 14 Maschinenteil; 15 Schmiermittel; 16 einfaches Boot; 18 it Vulkan; 19 ***Flächenmass***; 20 Wintersportgerät; 21 absurd; 23 Kern von 18 waagrecht; 24 deutscher Flugpionier; 26 „***das Mass aller IT“***; 28 böse Tiere; 29 der schnelle Zug ist in England kalt; 31 meist mit Trinidad in einem Zug genannt; 34 leichte Normmaschine; 35 Flusslandschaft; 37 Pflanzenhülle; 38 besitzanzeigendes persönliches Fürwort; 40 ist des andern Nachtigall; 42 Unerklärliches; 44 König (frz); 46 macht; 49 nicht nah; 50 kurz für Nummero; 52 Liestal ist sein Hauptort; 54 ***eine der wichtigsten Messgrössen in der IT***; 57 Witz; 59 kurzer Schiedsrichter; 60 engl Sagenkönig; 61 Schicksal; 63 griechischer Buchstabe; 65 was übrigbleibt, wenn das Resultat positiv ist; 69 ehemaliger äthiopischer Fürstentitel; 71 für den Engländer eben nicht Ost, wenn See; 72 ***sollte bei 100% stehen*** (engl); 75 AZ der Konsulate; 76 schlangenförmiger Fisch; 78 diese ***Tätigkeit*** könnte auch als Veranstaltungen interpretiert werden; 80 Onkel (span); 82 einer der glücklosen nahöstlichen Hoffnungsträger; 84 Anerkennung; 86 Kletterpflanze; 88 Platz; 89 Lebenskraft; 92 intl Abkürzung einer jungen Währung; 94 König (it); 95 12 senkrecht ist böse durcheinander geraten; 96 nichts (frz); 97 pers Fürwort im Dativ; 98 starker Zweig; 99 Kosewort für Nancy; 100 AZ Türkei; 101 Schiffsmanöver; 102 Wortgefüge.

Senkrecht: 1 Hitlers Heimat; 2 ***Längenmass***; 3 Touchdown; 4 Körper; 5 Orientierungslauf; 6 amerikanischer Geheimbund (Abk); 7 Dampfbad; 8 kurzer Teilnehmer; 10 Staudamm; 11 stärker geneigt; 12 nicht oben; 13 gesperrtes Territorium; 15 in Ordnung; 17 Sean Connery, sozusagen; 20 tonloser Stab; 21 Halt; 22 Dehnlaut; 25 Nahrungsmittel; 27 geht bitsy-teeny-weeny voran; 30 schmal; 32 den Standort verändern; 33 nordischer Männername; 36 Milchverarbeitungsart (Abk); 39 Tal; 41 Windseite; 43 Städter (lat); 45 russischer Strom; 47 spanischer Küstenfluss; 48 Drall; 49 glücklich (it); 51 Rohstoff (engl); 53 ***soll so schnell wie möglich sein*** (das Schluss-d fehlt!); 55 eine Art Gesetz; 56 Eingang; 58 AZ Zürich; 62 frz Behältnis; 64 ungesäuerte Brotplätzchen; 66 Gesichtshaar; 67 hinein (engl); 68 Behörde; 70 treffsicherer Mann, auch Sicherheitsschalter; 73 brasilianisches Fussballidol; 74 Fortpflanzungszellen; 77 Hauptschlagader; 79 Mär (Mz); 81 Offizier; 83 Vorwort; 85 Gliedmasse; 87 Zeitbegriff; 90 Kosename für Maria; 91 Tinte (engl); 93 ausgestorbenes Wildrind; 97 Doktor; 98 Flussname aus der Innerschweiz.

Die Lösung liegt in den markierten Feldern. Dieses Wort ist auf einer Postkarte zu senden an M.F. Bretscher, Oberrenggstrasse 8, 8135 Langnau a/A. Lösungen werden auch entgegengenommen unter der e-mail-Adresse

genommen unter der e-mail-Adresse mbretscher@kpmg.com. Einsendeschluss ist der 20. Mai 2005.

If there are less than 5 answers, or the solution has not been found, the $US 50 go into the Watson Jackpot to be carried forward to the next issue. Watson: Each puzzle contains some anomaly that is to be detected. If correctly identified, the Watson Jackpot is broken and replenished with $US 50 for the next issue.

Lösungen aus Nr. 73

Sarbanes-Oxley-Rätsel:
OOOOONOOOOO

Waagrecht: 1 Manna; 5 Egede: 8 Abend; 12 lost; 14 plot; 15 TB; 17 ***vereinbaren***; 19 SA, 20 Tuba; 22 See; 23 Drin; 25 Ari; 26 kalt; 28 Trog; 31 tea; 32 Losone; 35 Urolog; 37 Ea; 38 ***interactive***; 39 EZ; 41 Spalt; 43 Eboli; 45 loro; 47 Abt; 49 Iren; 50 Lek; 52 ***Operation***; 55 Cer; 57 miel; 59 Rente; 60 Aren; 62 MS; 63 Blei; 64 Nana; 65 GL (Glarus): 67 Lee; 66 Sosse; 71 CTT; 73 Spanne; 76 Betrag; 78 Tage; 79 ***interne***; 83 Eibe; 84 elend; 86 Delta; 87 Unser; 88 nor; 89 garnieren; 90 TRN.

Senkrecht: 1 Motta; 2 NL; 3 Nova; 4 Ase; 6 Geist; 7 Debet; 8 ale; 9 Bond; 10 et; 11 Diana; 13 truant; 14 (a) priori; 16 burlap; 18 NE; 19 Siegel; 21 bio; 24 RTO; 26 ***Kontrollen***; 27 leer; 29 rute; 30 ***Governance***; 33 Silo; 34 ***Sarbanes***; 26 lebe!; 37 Esel; 40 Zier; 42 Alki; 44 ONCE; 46 OP; 48 TTT; 49 lo; 53 Eris; 54 jene; 56 eng; 58 Ebenen; 61 Ratten; 62 Masten; 66 lagern; 67 Lager; 69 orten; 70 Sorte; 72 trist; 74 palo; 75 ei; 76 BE; 77 aber; 80 NDR; 82 Eli; 82 Nar; 85 DG; 87 un.

Deutschland: Umriss BRD 2005

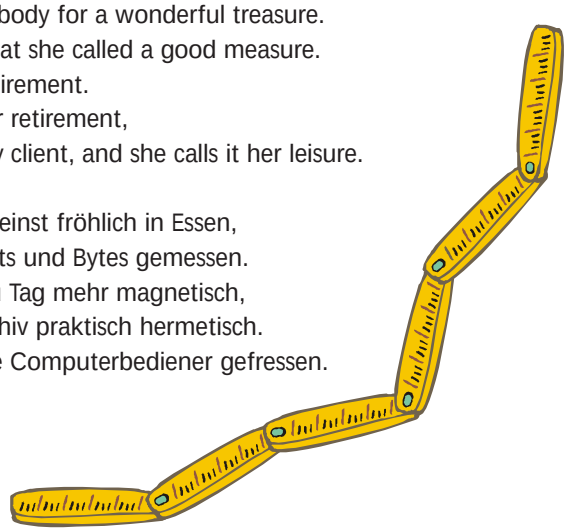
Waagrecht: 1 KA; 3 on; 4 Etui; 7 GS; 10 List; 11 Bora; 12 ***Seeenge***; 15 Abo; 16 ***Eck***; 18 R(o)hr; 19 CV; 20 Rache; 22 klebend; 23 Urne; 25 Beine; 26 Psi; 27 Ste; 29 Sn; 30 ni; 32 al; 33 Altane; 36 Seg; 38 Karosse; 41 baerenstark; 44 ***Bayern***; 46 ***Kiel***; 47 RM; 48 ear; 49 EF; 50 aer; 51 ***Hamb***; 53 ***urg***; 54 Sperre; 56 Alabaster; 59 Seraf; 61 est; 62 Los; 65 Ra; 65 Ern; 66 Pfeil; 69 LC; 70 Ferkel; 73 Eselsohr; 76 Mare; 77 Alaf; 78 CH; 79 Ex; 81 KT; 82 Dummheiten; 86 EM; 88 AAA; 89 ut; 90 Ainu; 92 Roux; 93 Ekar(te); 95 EE; 97 Bre; 98 ***Wende***; 100 Tester; 103 Ree; 105 CEO; 105 one; 107 wirklich; 110 Trense; 111 nie; 112 RG; 113 RF.

Senkrecht: 1 ***Koeln***; 2 Antigone; 5 use; 6 IT; 7 grèc; 8 ***Sachsen***; 9 ***Berliner***; 11 Born; 13 Ehen; 14 Erben; 15 Avus; 17 ***KE***; 21 aest; 22 Kessel; 24 ***RIAS***; 26 (Ex)plorers; 28 Tarife; 31 IKS; 32 Ara; 34 leb!; 35 errors; 37 gerast; 39 Ate; 40 ***Skagerrak***; 41 ***Bielefeld***; 42 Aera; 43 n(i)mmt; 45 Aepfel; 46 Kaa; 51 ha; 52 belch; 54 SA; 55 Ren; 57 Briefmarken; 58 ***RO***; 60 Raketen; 63 SF; 67 Esau; 68 ***LL***; 69 Lohe; 71 EM; 72 er; 74 schaust; 75 Retter; 80 Xe; 83 Mao; 84 Il; 85 ***Naa(b)***; 87 ***Muenchen***; 91 Irwein; 94 Kerker; 96 ***Ede***; 97 bring!; 99 EO; 100 Ton; 101 Set; 102 Ewer; 104 el; 108 RS; 109 ci.

Leider passierte ein Fehler bezüglich der Markierungen. Es hätten 12 „O“ sein sollen, das „N“ rutschte falsch hinein (von Marc Bucher aber richtig in der Lösung angegeben). Der beabsichtigte Watson war: Alle „O“ im Rätsel, die nicht auf einer Nummer sitzen. Die von Marc Bucher vorgeschlagene Watson-Lösung Aufschrei eines SOX-Projektleiters (oh, no!) ist so originell, dass das Redaktionsteam aus dem Jackpot weitere $US 50 „abliess“: Gesamtgewinn für Marc Bucher demnach $US 100 ISACA-Bookstore-Gutschrift. Herzliche Gratulation! Da niemand das zweite Rätsel mit dem Umriss der BRD meldete, verbleiben für die nächste Nummer $US 150 im Watson-Jackpot.

An old audit bag held her body for a wonderful treasure.
No man could produce what she called a good measure.
She had her stringent requirement.
And when she reached her retirement,
She now does it with every client, and she calls it her leisure.

Ein Computerrevisor lebte einst fröhlich in Essen,
Er hat sich tatsächlich in Bits und Bytes gemessen.
Er selber wurde von Tag zu Tag mehr magnetisch,
Verschloss sich im Bandarchiv praktisch hermetisch.
Und hat seither auch keine Computerbediener gefressen.



DACH-News

D: Aktivitäten des German Chapters

Das herausragende Ereignis der letzten Monate war wie jedes Jahr die Mitgliederversammlung des ISACA German Chapter am 11. März im Frankfurter Hilton Hotel. In diesem Jahr wurde wieder nach zweijähriger Amtszeit ein neuer Vorstand für die kommenden zwei Jahre gewählt.

Mehr als 40 Mitglieder haben die Mitgliederversammlung in diesem Jahr besucht. Am Vormittag startete die Veranstaltung zuerst mit einem Vortrag von Herrn Reinhold Kern zum Thema „Die Bedeutung von IT-Daten für den EDV-Prüfer im Fraud-Fall". Nach der Beantwortung und Diskussion von Fragen zum gehörten Vortrag setzten sich die Gespräche beim folgenden Mittagessen im Hotel fort.

Auf der am frühen Nachmittag beginnenden Jahresmitgliederversammlung wurden die Vereinsaktivitäten des letzten Jahres sowie die angedachten Vorhaben durch den Vorstand präsentiert. Der bisherige Vorstand wurde für das abgelaufene Jahr entlastet. Aus dem bisherigen Vorstand schied das Vorstandsmitglied Michael Schneider auf eigenen Wunsch aus. Nach der Aufnahme etwaiger Anwärter für die vorhandenen Vorstandsposten wurden die verbleibenden Vorstandsmitglieder in offener Wahl erneut bestätigt. Für den Vorstandsposten CISA-Koordination wurde Herr Holger Klindtworth in den Vorstand gewählt und nimmt somit den Platz von Herrn Schneider ein. Der neue Vorstand für die kommenden zwei Jahre ist auf den Seiten des German Chapter unter www.isaca.de wiederzufinden. Abgerundet wurde die Mitgliederversammlung mit einem Update zum Thema Linux Arbeitsgruppe, der Herr Neuy vorsteht sowie einem Ausblick auf zukünftige CobiT Entwicklungen. Das Protokoll der Mitgliederversammlung wird demnächst noch separat an alle Mitglieder versandt.

An dieser Stelle möchten wir natürlich auch unserem ausgeschiedenen Vereinsvorstand Herrn Michael Schneider ganz herzlich danken. Herr Schneider hat sich über viele Jahre direkt im Vorstand in unterschiedlichen Ressorts zuletzt als CISA-Koordinator engagiert und den Verein all die Jahre aktiv mitgestaltet. Wir hoffen natürlich alle, dass er uns weiterhin als aktives Mitglied im ISACA German Chapter erhalten bleibt und wünschen ihm weiterhin alles Gute.

Die Mitgliederentwicklung mit 760 Mitgliedern zum 31. Dezember 2004 sowie die Kassensituation des Vereins sind sehr erfreulich. Dies ermöglicht dem German Chapter auch die Unterstützung aktiver regionaler Arbeitsgruppen sowie der Workgroups z.B. zum Thema Linux. Weitere Informationen zu Arbeitsgruppen oder Workgroups sowie die Unterstützung durch das German Chapter lassen sich über Herrn Wojtyna erfragen.

Die diesjährigen CISA-Vorbereitungskurse des German Chapters werden in Hamburg und Frankfurt ab April stattfinden. Die Struktur in Form von Wochenendseminaren an jeweils zwei Wochenenden und einem abschließenden CISA-Testexamen hat sich nun im zweiten Jahr bewährt und wird beibehalten. Weitere Informationen auch für Nachzügler sind unter www.isaca.de zu finden.

Zum Schluss möchten wir noch alle Mitglieder dazu auffordern, den ***NewsLetter*** verstärkt als Basis für den Wissens- und Erfahrungsaustausch zu nutzen sowie die Möglichkeit in den neuen Workgroups mitzuarbeiten oder auch eine Workgroup ins Leben zu rufen zu nutzen, da der Berufsverband letztlich von den Aktivitäten seiner Mitglieder lebt.

Ingo Struckmeyer
Vorstand German Chapter

CH

ISACA Chapter Switzerland earns the 2004 K. Wayne Snipes award for the Best Very Large Chapter in Europe/ Africa!

Gute Neuigkeit traf Mitte Februar bei unserer Präsidentin ein. Die E-Mail kommend vom Chapter Relations Coordinator hatte folgenden Inhalt:

„On behalf of the Membership Board, I am pleased to extend congratulations to the Switzerland Chapter for an outstanding year in 2004. Your chapter has earned the 2004 K. Wayne Snipes award for the Best Very Large Chapter in Europe/Africa. The competition was very intense this year, and you should be extremely proud of the hard work your chapter put forth in order to earn this distinction.

The award will be formally presented to your chapter at the 2005 Global Leadership Conference in Las Vegas, Nevada, USA on 23-24 April 2005. The worldwide winner for each size category will not be announced until Sunday, 24 April.

Again, congratulations on a job very well done by your chapter board and your active members who have no doubt contributed significantly to this achievement."

Auch von dieser Seite einen herzlichen Dank an alle ISACA-Mitglieder, die sich für ein lebhaftes und interessantes Chapter-Leben einsetzen.

Vereinsversammlung des ISACA Switzerland Chapter

Am 17. März 2005 fand in Biel die 37. Vereinsversammlung des ISACA Switzerland Chapters statt. Daniela Gschwend konnte auf ein erfolgreiches Jahr für das Switzerland Chapter zurückblicken, wobei die Durchführung der EUROCACS im letzten Frühjahr ein wesentlicher Höhepunkt war. Nicht zuletzt der teilweise bedingungslose Einsatz der die Veranstaltung unterstützenden Mitglieder führte dazu, dass dem Chapter der „Verdienstorden" des besten grossen Chapters der Europa/Afrika Region 2004 zugesprochen wurde.

Die langsame Erholung der Wirtschaft schlug sich auch in der verbesserten Kursauslastung nieder. Dies wiederum hatte zur Folge, dass sich die finanzielle Lage des Vereins nach dem letztjährigen Rückschlag nachhaltig erholte. Die Teilnehmer stimmten deshalb auch dem stark auf Ausbildungsinvestitionen ausgerichteten Budget zu.

Der Posten des Vorstandsmitglieds für die Romandie ist verwaist, weil Paul Wang infolge Arbeitsüberlastung seinen Rücktritt einreichen musste. Seine Arbeit wurde verdankt und der Hoffnung Ausdruck gegeben, dass er weiterhin für die Führung der IG Forensic zur Verfügung steht. Die übrigen Vorstandsmitglieder wurden in globo mit Akklamation wiedergewählt.

Der neue Statutenentwurf wurde teilweise heftig diskutiert, ergänzt und verabschiedet. Die Änderungen waren insbesondere wegen der Einführung des Titels CISM nötig geworden. Daneben konnten einige „Unebenheiten" bereinigt werden.

Vor der Versammlung hielt Ivan Moss einen äusserst spannenden Vortrag mit reger Diskussion zum Thema ***The Rise and Fall of TXU Europe***. Die nächste Ausgabe des NewsLetters wird auf dieses „Juwel" eintreten. So viel sei verraten: Die Abwesenden haben etwas verpasst!

News aus den Interessengruppen

IG Operational IT-Risk

Peter R. Bitterli
Bitterli Consulting AG
Konradstrasse 1
8005 Zürich
Tel. + 41 1 440 33 60
Fax. +41 1 440 33 61
prb@bitterli-consulting.ch

Die IG hat im letzten Jahr den ersten Teil der Arbeiten abgeschlossen und will sich neu positionieren. Die IG wird 2005/06 eine Art „Kochbuch" für IT Risk Management erstellen und sucht dazu noch weitere Interessenten. Wir laden daher ein zu einer unverbindlichen Orientierungsveranstaltung am Mittwoch, den 25.5.2005, von 13:40–16:20 Uhr.

Da die IG-Veranstaltung in den Räumlichkeiten von ITACS Training stattfinden wird (5 Minuten vom Hauptbahnhof Zürich), besteht anschliessend an diesen Teil die Gelegenheit, von 16:40–17:40 Uhr das After Hour Seminar von ISACA zum Thema „Sicherheit in gehosteten Voice-over-IP Lösungen" zu verfolgen.

Anmeldung bitte bis 20.5.2005 an prb@bitterli-consulting.ch.

IG Government IT-Audit („Closed user group")

Michel Huissoud, CISA, CIA
Eidg. Finanzkontrolle/
Contrôle fédéral des finances
Monbijoustr. 45
3003 Bern
Tel. +41 31 323 10 35
Fax. +41 31 323 11 00
Michel.Huissoud@efk.admin.ch

La participation à ce groupe est réservée aux collaborateurs des organes de contrôle.

IG Computer Forensics

Paul Wang
PricewaterhouseCoopers
Avenue Giuseppe-Motta 50
1211 Geneva 2
Tel. +41 22 748 56 01
Fax. +41 22 748 53 54
Mobile: +41 79 220 54 07
Paul.Wang@ch.pwc.com

L'objectif de ce groupe de discussion lié aux « Computer Forensics », est de fournir un forum d'intérêt et d'information sur les méthodologies et les outils de ce qu'on appelle communément en français « Assistance informatico-légale ». Ce forum offre

la possibilité de partager des idées, des technologies, des outils et certainement aussi des notions juri-diques de ce domaine en constante évolution. Ce groupe de discussion abordera également des discussions techniques et procédurales sur les prérequis en matière de recherche de preuves informatiques. Même si les participants doivent être familiers avec la recherche, l'acquisition et l'analyse de preuves informatiques, tous les intéressés de tout niveau de connaissance sont les bienvenus.

IG Einführung von IT-Governance

Rolf Merz
Ernst & Young AG
Brunnhofweg 37
Postfach 5032
3001 Bern
Tel. +41 58 286 66 79
Fax. +41 58 286 68 27
rolf.merz@ch.ey.com

Nächste Sitzung: Voraussichtlich April/Mai
Weitere Interessenten können sich bei Rolf Merz anmelden.

Traktanden:
1. Präsentation der beiden Pilotprozesse PO1 und PO10
2. Festlegen Weiteres Vorgehen
Themen, Ziele und Organisation der nächsten Sitzung

IG Romandie

Vacant : touts personnes intéressées à participer ou animer un groupe de travail ou tous ceux qui aimeraient proposer un thème de réflexion peuvent s'annoncer auprès de M. Paul Wang.
paul.wang@ch.pwcglobal.com

IG Outsourcing/Insourcing

Ulrich Engler
Swiss Life
CF/REV HG 3151
General-Guisan-Quai 40
Postfach, 8022 Zürich
Telefon +41 43 284 77 58
Telefax +41 43 284 47 33
ulrich.engler@swisslife.ch

Nächste Sitzung: Offen. Interessenten melden sich bei Ueli Engler.

Mögliche Themen: Kontiniuität des Insourcers, Abhängigkeit vom Insourcer (Konkurs), Überarbeitetes Rundschreiben EBK, Fernwartung, etc.

IG MIS/EIS/DWH

Leitung:
Daniel Oser
Ernst & Young AG
Badenerstrasse 47
Postfach 5272
8022 Zürich
Tel. +41 58 286 34 39
Fax. +41 58 286 32 76
daniel.oser@ch.ey.com

Nächste Sitzungen: Mittwoch, 30. März 2005, 09.30 bei Ernst & Young AG, Bleicherweg 21, Zürich
Traktanden:
- Wrap-Up/Standortbestimmung
- Weiteres Vorgehen
- Wahl des neuen IG-Leiters
- Diverses

ev. gemeinsames Mittagessen

Neue Interessenten können sich bei Daniel Oser, IG-Leiter, anmelden.

IG SAP R/3

Monika E. Galli Mead
Eidg. Finanzkontrolle
Monbijoustrasse 51a
3003 Bern
Tel. +41 31 324 9495
Fax. +41 31 323 1101
monika.galli@efk.admin.ch

Nächste Sitzung: 28. April 2005 in Basel
Neue Interessenten können sich bei Monika Galli, IG-Leiterin, anmelden.

Information Systems Audit and Control Association®
www.isaca.ch

Achtung wichtig!

Das ISACA-Kurssekretariat ist ab 14. März 2005 unter der folgenden Adresse erreichbar:

ISACA Switzerland Chapter
Kurssekretariat
c/o ITACS Training AG
Stampfenbachstrasse 40
CH - 8006 Zürich
Tel +41 (0)44 444 11 01
Fax +41 (0)44 444 11 02

Veranstaltungen

Intensivkurs Datenschutzgesetz und dessen Umsetzung	11. April 2005 Zürich, 1 Tag, Infosec
CobiT User Convention	11.–12. April 2005 TBA (Europa), 2 Tage, ISACA USA
Verhalten in Konfliktsituationen	21. April 2005 Zürich, 1 Tag, Infosec
Internet Security Lab – Workshop mit Angriffsszenarien und Abwehrmassnahmen	20.–22. April 2005 Zürich, 3 Tage, ISACA CH/Compass
After Hour Seminar (AHS): SOX IT in Novartis	27. April 2005 Zürich, 16.40 Uhr, ISACA CH
Service Management - ITIL Foundation Training – Auf der Basis de facto-Standards ITIL mit Links zur BS 15000 Zertifizierung	2.–4. Mai 2005 Zürich, 3 Tage ISACA CH/glenfis
Evidence Lab – Workshop über die Spurensuche in Computersystemen	11.–13. Mai 2005 Zürich, 3 Tage, ISACA CH/Compass
Audit & Control of Information Technology & Systems	17./18. Mai 2005 London, 2 Tage, MIS
Wireless-LAN-Sicherheit	20. Mai 2005 Zürich, 1 Tag, Infoguard
Fraud Bootcamp	23.–27. Mai 2005 Genf, 5 Tage, MIS
After Hour Seminar (AHS): Sicherheit in gehosteten Voice-over-IP Lösungen	25. Mai 2005 Zürich, 16.40 Uhr, ISACA CH
ITIL Business Continuity and IT Service Continuity – Von Business Continuity zur IT Disaster Recovery auf der Basis des de facto-Standards ITIL	26.–27. Mai 2005 Zürich, 2 Tage, ISACA CH/glenfis
IT-Tagung 2005	30./31. Mai 2005 Frankfurt aM, 2 Tage, IIR Akademie / ISACA
Anwendungssicherheit: Risikoorientierte Entwicklungsmethoden	6.–8. Juni 2005 Zürich, 3 Tage, ITACS Training AG
Zutrittskontrolle im Spannungsfeld der Systemintegration	9. Juni 2005 Zürich, 1 Tag, Mediasec
2nd Annual CISO Executive Summit	16./17. Juni 2005 Genf, 2 Tage, MIS
International Conference	19.–22. Juni 2005 Oslo, 4 Tage ISACA
Prüfung von Schnittstellen/Audit des Interfaces	30. Juni 2005 Bern, 1 Tag, ISACA/Kammer

Information Systems Audit and Control Association

Kontaktadressen Veranstalter

Der ***NewsLetter*** empfiehlt folgende Veranstalter (weitere Kurse und Unterlagen direkt anfordern):

AFAI
Tel. +33 1 55 62 12 22
afai@afai.asso.fr
www.afai.asso.fr

advanced technology seminars
Grundgasse 13
CH-9500 Wil
Tel. +41 71 911 99 15
Fax. +41 71 911 99 16
Maurer@inf.ethz.ch

Stiftung für Datenschutz und Informationssicherheit
Dr. Beat Rudin
Kirschgartenstrasse 7
Postfach
CH-4010 Basel
Tel. +41 61 270 17 70
Fax +41 61 270 17 71
beat.rudin@privacy-security.ch
www.privacy-security.ch

e-tec Security
PO Box 54
Wilmslow Chesire SK9 6FU
United Kingdom
info@a-tecsecurity.com

Euroform Deutschland GmbH
Hans-Günther-Sohl-Strasse 7
D-40235 Düsseldorf
Tel. +49 211 96 86 300
Fax. +49 211 96 86 509
info@euroforum.com

Hochschule für Technik Rapperswil
Institut für Internet Technologien und Anwendungen
Oberseestrasse 10
8640 Rapperwil
Tel. +41 55 222 41 11
Fax. +41 55 222 44 00
office@hsr.ch

IIR-Akademie
Ohmstr. 59
D-60468 Frankfurt/Main
Tel. +49 69 7137 69-0
Fax. +49 69 7137 69-69
iir.academie@iir-ev.de

InfoGuard AG
Feldstrasse 1
CH-6300 Zug
Tel. +41 41 749 19 00
Fax +41 41 749 19 10
www.infosec.com

Integralis GmbH
Gutenbergstr. 1
D-85737 Ismaning
Tel. +49 89 94573 447
Fax +49 89 94573 199 fx
schulung@integralis.de

ISACA CH
Kurssekretariat
c/o ITACS Training AG
Stampfenbachstr. 40
8006 Zürich
Tel. +41 44 444 11 01
Fax. +41 44 444 11 02
info@isaca.ch

ISACA USA
3701 Algonquin Rd #1010
USA_Rolling Meadows IL 60008
Tel. +1 847 253 15 45
Fax. +1 847 253 14 43
www.isaca.org

Marcus Evans
Weteringschans 109
1017 SB, Amsterdam
The Netherlands
Tel. +31 20 531 28 13
Fax. +31 20 428 96 24
www.marcusevansnl.com

MIS Training Institute
Nestor House
Playhouse Yard P.O. Box 21
GB-London EC4V 5EX
Tel. +44 171 779 8944
Fax. +44 171 779 8293
www.misti.com

MediaSec AG
Tägernstrasse 1
8127 Forch/Zürich
Tel. +41 1 360 70 70
Fax. +41 1 360 77 77
it@mediasec.ch

Secorvo Security Consulting GmbH
Secorvo College
Albert-Nestler-Strasse 9
D-76131 Karlsruhe
Tel. +49 721 6105-500
Fax +49 721 6105-455
info@secorvo.de
www.secorvo.de

Treuhand-Kammer
Jungholzstrasse 43
Postfach
CH-8050 Zürich
Tel. +41 1 305 38 60
Fax. + 41 1 305 38 61

ZfU Zentrum für Unternehmensführung AG
Im Park 4
CH-8800 Thalwil
Tel. +41 1 720 88 88
Fax. +41 720 08 88
info@zfu.ch

Vereinsadressen

Germany Chapter

Geschäftsstelle
ISACA e.V., German Chapter
Eichenstr. 7
D-46535 Dinslaken
Tel. +49 2064 733191
isaca.dinslaken@t-online.de

Präsidentin
Karin Thelemann
Tel. +49 6196 99626 488
karin.thelemann@de.ey.com

Konferenzen
Markus Gaulke
Tel. +49 69 9587 2313
MGaulke@kpmg.com

Mitgliederverwaltung und Kassenwart
Norbert Gröning
Tel. +49 201 438 0
Norbert.Groening@de.pwcglobal.com

Public Relations
Heinrich Geis
Tel. +49 692 101 5149
heinrich.geis@deutsche-boerse.com

Arbeitskreise und Facharbeit
Bernd Wojtyna
Tel. +49 251 288 4253 oder
+49 251 210 4539
bernd_wojtyna@gmx.net

Publikationen
Ingo Struckmeyer
Tel. +49 4106 704 2336
ingo.struckmeyer@pf.comdirect.de

CISA-Koordinator
Holger Klindtworth
Tel. +49 (40)41522863
h.klindtworth@susat.de

www.isaca.de

Austria Chapter

Vorsitzender (Präsident)
Ing. Mag. Dr. Michael Schirmbrand
Tel: +43 1 31332 656
m.schirmbrand@kpmg.com

Stellvertretender Vorsitzender I (Vizepräsident I)
Dipl.-Ing. Maria-Theresia Stadler,
Tel: +43 1 53127 2857
maria-theresia.stadler@oekb.at

Stellvertretender Vorsitzender II (Vizepräsident II)
Mag. Josef Renner
PricewaterhouseCoopers
Tel: +43 1 501 88 1701
josef.renner@at.pwcglobal.com

Schriftführer, Mitgliederversammlung, Marketing
Mag. Gunther W. Reimoser
Tel: +43 1 12 111 701 032
gunther.reimoser@at.ey.com

Kassier, Webmaster
Mag. Jimmy Heschl
Tel: +43 1 31332 619
jimmy@heschl.at

CISA/CISM-Koordinator
Mag. Ulrike Knödlstorfer-Ross
Tel: +43 1 33151 145
ulrike.knoedelstorfer@ama.gv.at

NewsLetter-Koordination
Mag. Dieter Stangl-Krieger
Tel: +43 1 31332 619
DStangl-Krieger@kpmg.at

E-Mail ISACA Austria Chapter:
office@isaca.at

www.isaca.at

Switzerland Chapter

Präsidentin
Daniela S. Gschwend
Tel. +41 43 285 69 36
daniela_gschwend@swissre.com

Vizepräsident
Michel Huissoud, CISA, CIA
Tel. +41 31 323 10 35
Michel.Huissoud@efk.admin.ch

Kassier
Pierre A. Ecoeur, CISA
Tel. +41 71 626 64 61
pierre-alain.ecoeur@tkb.ch

Ausbildung/Kurssekretariat
Peter R. Bitterli, CISA
Tel. +41 44 444 11 01
prb@bitterli-consulting.ch

CISA/CISM-Koordinator
Thomas Bucher
Tel. +41 44 421 64 22
tbucher@deloitte.com

Sekretär
c/o Präsidentin

Information & Kommunikation
Monika Josi
Tel. +41 61 697 72 41
monika.josi@ah.novartis.com
Adressmutationen bitte hier melden.

Koordinator Interessengruppen
Rolf Merz
Tel. +41 58 286 66 79
Rolf.Merz@ch.ey.com

Représentant Suisse Romande
Paul Wang
Tel. +41 22 748 56 01
paul.wang@ch.pwcglobal.com

Marketing
Bruno Wiederkehr
Tel. +41 1 910 96 33
bru.wiederkehr@bluewin.ch

www.isaca.ch