



Information
Security Society
Switzerland

> *vormals FGSec*

Revisionskonformes Information Security Management für ERP-Systeme

Luzern 30. September 2008

Forum 3: Die verschiedenen Aspekte der
ERP Prüfung – Anforderungen und Nutzen
der Revision

Teilnehmer

- Robert Borja, ISSS / PWC, Chair
- Marcus Holthaus, IMSEC, Co-Chair
- Jürgen Müller, Systems & Process Assurance
Leader Switzerland, Partner
PriceWaterhouseCoopers
- Pascal Reiniger, Informatik Revisor, Coop
- Volker Lehnert, Consultant Fachbereich Security,
SAP Schweiz
- Jörg Altmeier, Geschäftsführer, wikima4

Fragestellungen

- **Wie kann ich mit 10 SAP_ALL noch revisionskonform bleiben?**
- Welchen Nutzen haben Unternehmen aus ERP Prüfungen gezogen?
- Wie wird ein adäquates Risikomanagement bei ERP-Systemen ausgestaltet?
- **Was können Werkzeuge zur ERP-Sicherheit beitragen?**

Fragestellungen aus dem Publikum (Plenum vor der Gruppendiskussion)

- Ist es sinnvoller Fehlbuchungen zu korrigieren oder Fehlverbuchungen stehen zu lassen und „besser“ weiterzumachen?
 - Beide Lösungen möglich
- Werden Ex-Post-Kontrollen auf die Dauer nicht ziemlich teuer?
 - Ja, mittelfristig braucht es aber ein Projekt
 - Zu viele Compliance-orientierte Projekte statt Business-Orientierung
- Gibt es formelle Anforderungen an die nachträgliche Erstellung eines PO (Product Order) z.B. beim Wareneingang?
 - Schweirige Frage. Grundsätzlich ist Treue zum Business relevant; „es muss gebucht worden sein, wenn kontrolliert wird“

Diskussion IKS

- Was kann ich konkret aus IT-Security Sicht einbauen um die IKS-Bestrebungen zu unterstützen?
 - Prüfung nach ISO 27000 (nicht nur Zugriffsschutz);
- Fokussierung der IT-Sicherheit in diesem Bereich:
 - Risiken, welche die finanzielle Berichterstattung beeinflussen
 - Kernbereiche Zugriff und Change Management
 - Aus Standard 890...
 - **Sicherheit: Authorisierung, Testen und Implementieren von Zugriffsrechten**
 - **Change Management**
 - **Development von neuen Operationen**
 - **Operations /Betrieb**
 - Wenn man auf IKS-Konformität ist:
 - „nicht überbauen“
 - Man kommt mit relativ wenigen Kontrolle zur Konformität

Diskussion IKS

- **Es gibt Tools die das unterstützen**
 - Inhalte kommen aus Arbeitskreisen, u.a. „Organisation und Risk Management“, es werden Handbücher geschrieben die alles benötigen um eine interne Prüfung durchzuführen-
 - Inhalte können in Tools integriert werden?
- Es kommt aufs **Betriebsführungskonzept** an
 - Welche generellen Risiken und Controls sind möglich und notwendig?
 - Was ist als automatisierte Kontrolle möglich und was
 - Im Solution Manager sind Netzwerkzugriffe kontrollierbar etc.
 - Es gibt also technische Kontrolle von Basis bis zu übergreifendem IKS (Schwerpunkt financial controls)
- Revisoren-Antwort: „Es kommt drauf an“
 - Geht es um die **Durchführung und Form der Prüfung oder geht es um das IKS...**
 - Bei Coop v.a. Beschäftigung mit IKS
 - Wesentliche Frage: „Was ist IKS in der Informatik?“ **Bei fast allen Prüfungen werden Informatiker involviert**

Diskussion IKS

- Es gibt viele, zu viele Prüfpunkte -> wichtig ist zu definieren wer für was verantwortlich ist und sauber abzugrenzen, gleichzeitig sicherzustellen dass nichts zwischen Stuhl und Bank fällt.
- Erst dann Untersuchung der Risiken und der möglichen Massnahmen
- Ausgangsbasis bei Coop war **ITIL**, aber einzelne Prozesse weichen stark von ITIL ab. Beobachtungsprozess ist immer der Informatik-Prozess, und wir betrachten dann im Detail die Eigenschaften der Prozesse, und identifizieren die Risiken, z.B. „Autorisierungen per Telefon“; am Schluss – geht man davon aus – man sei automatisch revisionskonform
- **Zentral ist wenn ein Prüfer kommt „dass man erklären kann“ und nicht einfach ein Standard-Buch hinwirft...**

Diskussion IKS

- Nach OR wird von den Finanzzahlen ausgegangen; dann wird das auf die Prozesse und Systeme heruntergebrochen;
- Wenn in den Systemen Appliationskontrollen enthalten sind, dann muss man sich darauf verlassen können
- **Z.B. bei „Desaster Recovery nach ...“ wird eher ausgeklammert; Business Continuity Planning ist selten zentral bei Revisionen**
- **Ziel ist, das eigene IKS für sich selbst zu leben (einen Nutzen daraus zu ziehen); und conform zu sein**

Diskussion IKS

- Spannend ist sich nicht nur auf die einmalige Prüfung auszurichten (v.a. Auf die nächste), sondern einen kontinuierlichen Prozess aufzubauen und Kontinuität aufzubauen
- Es gibt viele Möglichkeiten und Tools für die Prüfung und für die laufenden Kontrollen
- Bei der Erstellung von Revisionsberichten wird oft relativ viel Zeit verbraucht, weil die Prüfer oft wechseln oder „jedes Jahr dasselbe erklärt werden muss“; oft werden viel zu viele Controls definiert und auch noch implementiert.
- Der Process Owner weiss wo die Controls sind weil er den Prozess kennt und weiss welche Daten in den Systemen sind; das kann man nicht einfach von aussen aufsetzen
- Revisoren sind da damit die eigenen Prozesse optimiert werden, nicht nur um zu kontrollieren. Eigenkontrolle und Selbst“bewusstsein“ der Systeme wird wichtiger;

Diskussion IKS

- Je weniger die Organisation die eigenen Prozesse und das eigene IKS im Griff hat, desto aufwendiger ist die Revision, weil der Revisor seine Prüfung signieren muss und daher alles „genau“ wissen will
- ITCG = IT Corporate Governance
- Nachholende Kontrollen... wenn 97% der MA SAP_ALL haben, muss fast alles im Detral nachvollzogen werden

Diskussion IKS

- Es ist heute sehr schwierig, die Grundanforderungen an das IT-System festzustellen; welche Minimalanforderungen gelten? Es gibt eine Meinung pro Revisionsorganisation (3 externe und 1 interne)
- Antwort: Sie selbst bestimmen wo die Messlatte ist, und dann muss der Prüfer argumentieren, warum die Latte zu tief ist.
- Externe Prüfung muss „nur“ sicherstellen, dass die Geschäftszahlen im Geschäftsbericht im Wesentlichen korrekt wiedergegeben sind, mit möglichst kleinen Abweichungen
- Die „Übersetzungsarbeit“ von Grundanforderungen auf konkrete SAP-Controls muss jede Unternehmung selbst vornehmen; es gibt Ansätze für „Best Practices“ aber die Arbeit ist noch nicht abgeschlossen, daher ist jede Organisation selbst gefordert. Die meisten Organisationen orientieren sich an der eigenen Branche und den Branchenleadern.

Diskussion IKS

- Man kann die wesentlichen Controls schnell und gut auf eine kleine Anzahl reduzieren, wenn diese qualitativ hochwertig umgesetzt werden
- Bis 2007 war gar nicht wirklich klar wie man die gültigen gesetzlichen Vorgaben wirklich überprüfen kann. Es wurde dann von der schweizerischen Treuhandkammer diskutiert ob die Zunahme im Umfang der IKS eher heisst ob man sich darauf besser verlassen kann (d.h. Der externe Prüfaufwand sinkt) oder dass mehr gerüft werden muss weil mehr geregelt ist (d.h. Der externe Prüfaufwand steigt)
- Ziel müsste im Prinzip sein, dass die externe Revision „relevante, aber kleine Mängel“ findet.

Diskussion IKS

- Auch in einem Konzern – wie Coop – gibt es ganz unterschiedliche Bereiche, z.B. zwischen Interdiscount und Food Retail
- Es ist überraschend wieviel Security Anforderungen in CH gegenüber z.B. USA für eine börsenkotierte Gesellschaft gelten
- Die ganzen Frameworks sind immer auch deshalb schwammig weil sie für alle Branchen gelten sollen. Wie oft z.B: soll ein Passwort gewechselt werden? „Regelmässig“, aber wie oft? Was ist die best practice? Coop hat von „nie“ auf 180 Tage reduziert
- Es sind nicht die Revisionsgesellschaften, die das IKS erfinden; die Unternehmung kann selbst bestimmen wie das IKS aufgebaut werden soll
- Wichtig ist der Dialog bei der Bestimmung der „Schärfe der Massnahmen“. Meist kann man mit sehr wenigen Controls die Anforderungen erfüllen
- Kreativität und Intelligenz ist erforderlich, wenn es darum geht die richtigen Controls auszuwählen und richtig umzusetzen

Diskussion IKS

- Bei jeder Organisation gibt es einen anderen Kontext; Trader, die ihren Arbeitsplatz verlassen, brauchen eine andere Screen Saver Policy als Fließbandarbeiter
- Die Revisoren haben Einfluss auf die Best Practice; Eine Best Practice kann man immer diskutieren, aber man muss das auch tun,
- Das Tool darf natürlich nicht wichtiger werden als der Content
- Best Practices enthalten nicht eine finale Wahrheit
- Verschiedene Branchen fangen nun an, sich untereinander abzustimmen, z.B. Energie-Branche etc.; das kommt jetzt weil die Unternehmen aufgrund der gesetzlichen Regelungen jetzt (seit zwei Monaten) den Eindruck haben, etwas tun zu müssen; Ende Jahr muss etwas vorliegen
- Auch Migros diskutiert mit Coop über notwendige Level

Diskussion „10 SAP_ALL“

- SAP_ALL heisst alle Berechtigungen im System
- Damit das revisionskonform ist muss ein Superuser Control aktiviert sein; jeder Superuser Zugriff muss protokolliert werden; man kann also compliant sein, aber das ist sehr aufwendig weil die Logs kontrolliert und interpretiert werden müssen
- In jedem produktiven System braucht es minimal einen SAP_ALL Account; SAP_BASE genügt für Standard-Maintenance
- Alternative Aussage: Auf einem produktiven System darf kein SAP_ALL enthalten sein, da es Revidierbarkeit brechen kann; es darf auch temporär keinen brauchen. SAP_ALL darf zwar definiert werden, aber muss im Safe liegen und nur bei grosser Systemstörung verwendet werden.
- Auch bei vielen SAP_ALL kann man noch Konsolidierungen / Korrelationen mit vor- und nachgelagerten Systemen durchführen, um Plausibilität

Diskussion „SAP_ALL“

- SAP_ALL wird oft an die Informatiker vergeben, typischerweise nicht an Business-User. Wegnahme von SAP_ALL kann aber das Business brechen, daher muss eine konsequente Ablösung als Projekt angegangen werden
- Bei der Beschäftigung mit den Tools stellt man fest dass es verschiedene Möglichkeiten gibt, Rechtevergabe zu prüfen, auch automatisiert.
- Immer mehr Systemadmins sagen „ich will SAP_ALL gar nicht mehr“, weil sie die Verantwortung aufgrund zunehmender Awareness nicht mehr möchten; mit ein bisschen „Sniffing“ kann man die Awareness stark erhöhen. -> Schutz des Users vor „sich selbst“ und unbeabsichtigtem Fehlverhalten
- Ergo: meist ist die Reduktion der SAP_ALL-User-Anzahl möglich.

Diskussion „SAP_ALL“

- Pragmatische Lösung:
 - SAP_ALL wird kopiert z.B. in Z_ALL
 - SAP_ALL wird so weit wie möglich entfernt
 - Z_ALL bleibt verteilt, aber Nutzung wird geloggt und der Nutzung wird nachgegangen; Nutzung muss aber in Notfällen unkompliziert möglich sein um grössere Schäden zu verhindern; einzelnen Usern muss man sowieso vertrauen!
- „Wenn jemand ein System zerschliessen will, dann kann er das.“

Company Wide Controls: Sicherheitsverständnis

- Z.B. Vorfall der Durchführung von Test in Produktionsumgebung; wie kann sichergestellt werden dass alle Testfälle wieder von Produktion entfernt werden
- Erkenntnisse aus der Praxis: Controls hin oder her: Die User lernen mit der Zeit das System zu überlisten und so zu nutzen dass es den eigenen Anforderungen genügt
- Es besteht ein Mangel an Skill einzelner Business Process Owner; der (interne) Revisor hat auch eine Awareness-fördernde oder auch eine Ausbildungsaufgabe; (interner) Revisor ist auch Coach

Trennung von Produktion und Integration?

- Umfrage bei Teilnehmern: Wer trennt Produktion von Integration der Informatik (nicht nur SAP) etc.?
 - ca. 80%
- Wer trennt weiter, z.B. Integration von Test/Schulung?
 - ca. 60%
- Wer trennt weiter, z.B. Test und Schulung?
 - ca. 40%
- Wer trennt noch weiter, hat also 4 ähnliche Systeme im Einsatz?
 - ca. 20%

Summary - Podium3

- Es ist *Ihr* IKS,
 - Sie bestimmen
 - Es geht um kontinuierliche Selbstkontrolle
 - Sie sollten erklären können
- Es geht um Finanzzahlen aus dem Business und deren Nachvollziehbarkeit
- Vier wesentliche Kontrollbereiche:
 - Zugriffsrechte
 - Change Management
 - Development von neuen Operationen
 - Operations /Betrieb
 - Auch mit (kontrolliertem!) SAP_ALL kann man revisionskonform sein
 - Umfrage der Trennung von Stages (Produktion etc.)