

Prozesshandbuch der IT Audit Solution Group

**Beschreibung des von der IT
Audit Solution Group verwendeten
Revisionsprozesses**

BearbeiterIn:
Michael Meli
Senior IT Audit Manager

SYSTOR AG
Baslerstrasse 60
CH-8048 Zürich
Telefon +41 1 405 31 11
Telefax +41 1 405 31 13
www.systor.com

Zürich, 9. Januar 2001
©SYSTOR AG/Version 1.0

Inhaltsverzeichnis

| | |
|---|-----------|
| Management Summary | 4 |
| 1. Einführung | 5 |
| 1.1. Zielsetzung | 5 |
| 1.2. Flowchart Revisionsprozess | 6 |
| 1.3. Dokumentation der Revision (Übersicht) | 7 |
| 1.3.1. Zielsetzung der Dokumentation | 7 |
| 1.3.2. Dokumentationstool | 7 |
| 1.3.3. Dokumentgruppen | 7 |
| 1.3.4. Vertraulichkeit der Dokumentation | 9 |
| 1.3.5. Detaillierte Darstellung des internen Dokumentenflusses | 10 |
| 1.3.6. Zeithorizont der Aufbewahrung | 13 |
| 2. Planung der Revision | 14 |
| 2.1. Übersicht Planungsprozess | 14 |
| 2.2. Übersicht der Planungsphasen | 15 |
| 2.3. Set Up des Audits und des Audit Programms in Auditor Assistant | 15 |
| 2.3.1. Eröffnung einer Revision | 15 |
| 2.3.2. Audit / Project / Activity / Summary (APAS) Dokument | 16 |
| 2.3.3. Audit Planning Memorandum (APM) | 16 |
| 2.4. Revisionsakte | 16 |
| 2.5. Kontaktnahme mit revidierten Stellen | 17 |
| 2.5.1. Audit Announcement Memorandum (AAM) | 17 |
| 2.5.2. Kick-off Meeting | 17 |
| 2.6. Revisionsprogramm | 18 |
| 2.6.1. Aufbau eines Revisionsprogramms in Auditor Assistant | 18 |
| 2.6.2. Übersicht der Struktur von Auditor Assistant | 19 |
| 2.6.3. Prüfungsumfang (Scope) / Zeitbudget | 20 |
| 2.6.4. Detailliertes Prüfprogramm (RCMs) | 20 |
| 2.6.5. Know-how und Tools | 21 |
| 2.6.6. Revisionsprogramme und Tools des Kunden | 21 |
| 2.7. Informationssuche | 21 |
| 3. Field Work | 23 |
| 3.1. Übersicht Prozessablauf Feldarbeit | 23 |
| 3.2. Erste Informationsbeschaffung | 24 |
| 3.3. Ausführen der einzelnen Audit Steps | 24 |
| 3.4. Das Workpaper | 25 |
| 3.4.1. Dokumentation der Feldarbeit | 25 |

| | |
|--|-----------|
| 3.4.2. Beurteilung des Prüfungshandlung | 27 |
| 3.4.3. Conclusion | 28 |
| 3.5. Das Finding Dokument | 29 |
| 3.5.1. Dokumentation des Findings | 29 |
| 3.5.2. Disposition der Findings | 30 |
| 3.6. Audit Finding Memorandum (AFM) | 31 |
| 3.7. Der Review Prozess | 31 |
| 3.8. Der Aproval Prozess | 32 |
| 4. Reporting | 33 |
| 4.1. Prozessübersicht | 33 |
| 4.2. Der Management Letter | 34 |
| 4.2.1. ML Draft for discussion | 35 |
| 4.2.2. ML Final Draft | 35 |
| 4.2.3. Definitiver Management Letter | 35 |
| 4.3. Report | 36 |
| 4.4. Fristen der Berichterstattung | 37 |
| 4.5. Nummerierung der IT ASG Dokumente und Revisionen | 37 |
| 4.6. Reporting nach den Reporting Standarts des Kunden | 37 |
| 5. Abschluss der Revision (Closing of Audit) | 38 |
| 6. Follow-up | 39 |



Management Summary

Dieses Dokument hat zum Ziel, den Revisionsprozess welcher die IT Audit Solution Group bei Revisionen Anwendet, zu beschreiben und verbindlich festzulegen. Weiter ermöglicht es neuen Mitarbeitern sich in kurzer Zeit mit dem Revisionsprozess vertraut zu machen und es kann auch als Nachschlagewerk benutzt werden.



1. Einführung

1.1. Zielsetzung

Das vorliegende Dokument sollte die folgende Zielsetzungen erfüllen:

- Dokumentation und Beschreibung des Standard Revisionsprozesses
- Dokumentation und Beschreibung der administrativen Vorgänge welche mit der Revisionstätigkeit in Zusammenhang stehen
- Einbindung von Auditor Assistant in den Revisionsprozess
- Einführung für neue Mitarbeiter in den Revisionsprozess
- Qualitätsstandards setzen
- Allgemeine Referenz zur Vorgehensweise

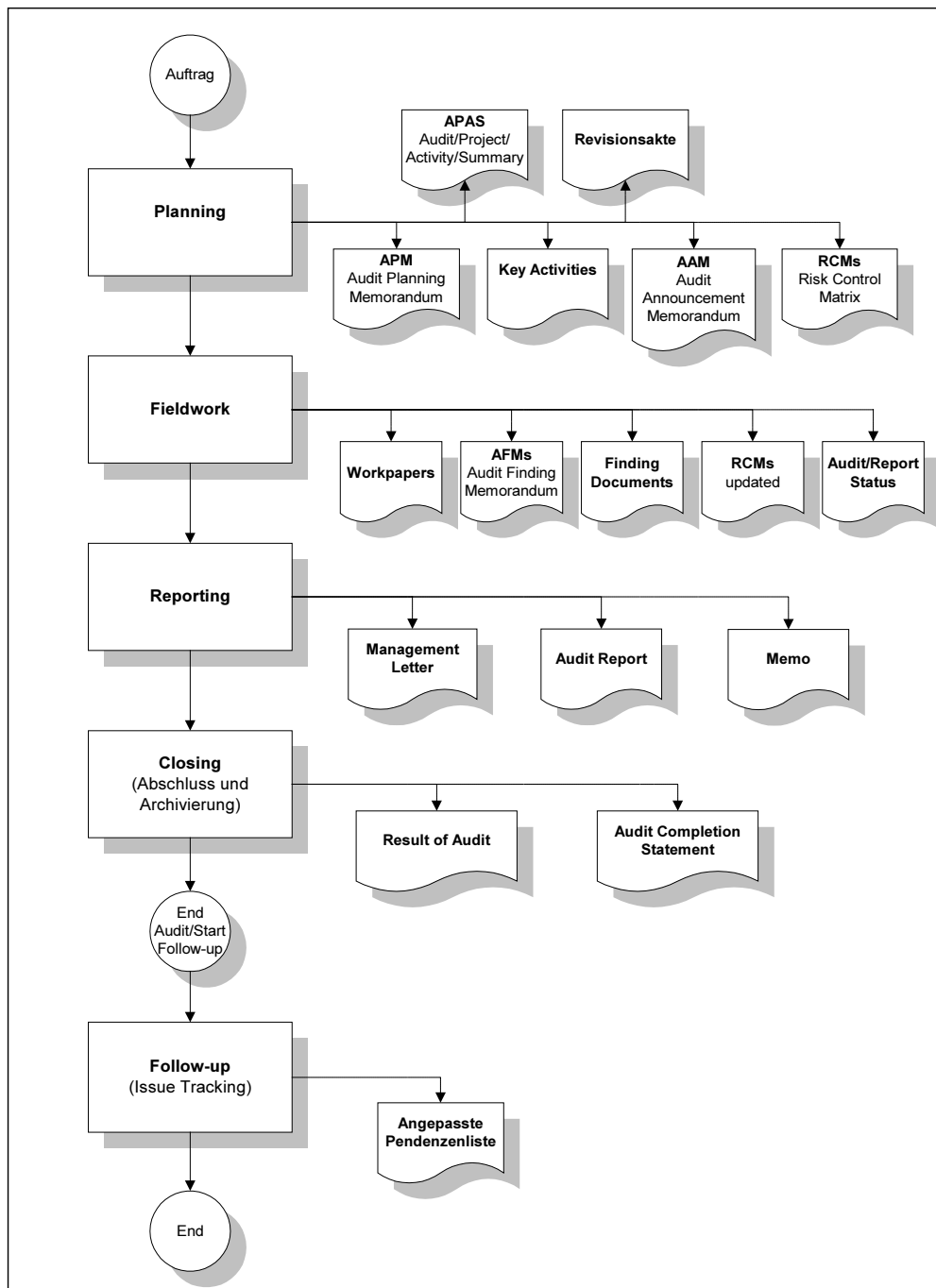
1.2. Gültigkeit

Das vorliegende Dokument ist für die von der SYSTOR IT Audit Solution Group geleiteten Revisionen verbindlich. Sollte der Kunde abweichende Wünsche haben, so sind diese vom Audit Manager zu dokumentieren und den Revisionsbeilagen beizufügen.

Im Fall eines Bodyleasings muss der betreffende Revisor sich streng an die Kundenvorgaben halten. Er kann selbstverständlich dieses Handbuch zur Orientierung verwenden, die Richtlinien des Kunden sind jedoch verbindlich anzuwenden und umzusetzen.

1.3. Flowchart Revisionsprozess

Untenstehende Grafik gibt einen schematischen Überblick über den Revisionsprozess und die resultierenden Dokumente in den einzelnen Prozessphasen. Eine ausführliche Beschreibung der Prozessphasen und der Dokumente erfolgt in den nachfolgenden Kapiteln zur Prozessbeschreibung.



1.4. Dokumentation der Revision (Übersicht)

1.4.1. Zielsetzung der Dokumentation

Ziele, welche durch eine qualitativ hochstehende und lückenlose Dokumentation der Revisionstätigkeit, erfüllt werden müssen:

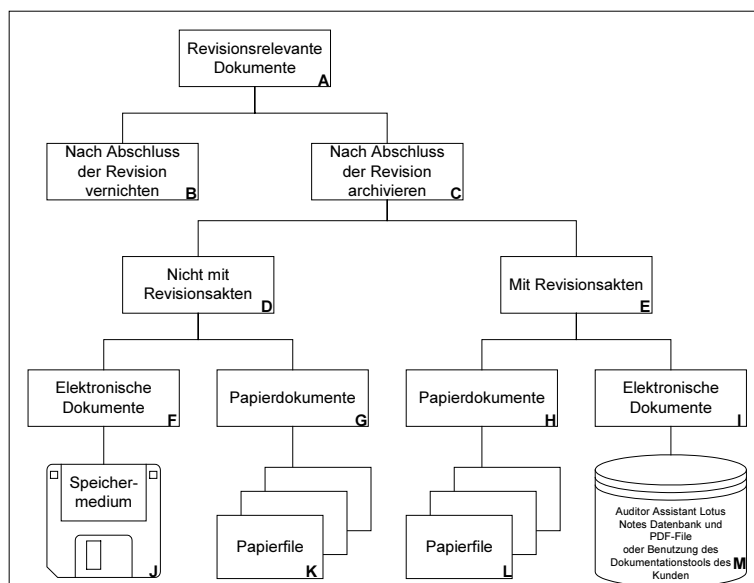
- Einhaltung der gesetzlichen Vorschriften (Nachvollziehbarkeit, Aufbewahrungspflicht 10 Jahre).
- Erstellung eines vollständigen Audit-Trails. Darunter ist sämtliche Dokumentation zu verstehen, welche benötigt wird, um die Art und den Umfang der vorgenommenen Prüfungen sowie die vorgefundenen Mängel mit den dazu gemachten Feststellungen zu belegen. Damit wird erreicht, dass Aussagen im Revisionsbericht (Audit Report) einer nachträglichen Überprüfung standhalten und nicht in Frage gestellt werden können.
- Möglichst wenig Papierdokumente, d. h. wenn möglich Dokumente in elektronischer Form speichern.

1.4.2. Dokumentationstool

Die IT Audit Solution Group setzt zur Dokumentation, zum Aufbau eines lückenlosen Audit Trails und zum Informationsaustausch innerhalb des Revisionsteams das auf Lotus Notes basierende Tool Auditor Assistant ein. Eine detaillierte Beschreibung der Prozesse und Gebrauchsanweisung für die Benutzung von Auditor Assistant befindet sich im Prozesshandbuch Auditor Assistant.

1.4.3. Dokumentgruppen

Das untenstehende Schema gibt einen Überblick über die **Dokumentgruppen im Revisionsprozess**. Eine ausführliche Beschreibung der Dokumente erfolgt in den Kapiteln zur Prozessbeschreibung.



Beschreibung der Dokumentgruppen

| # | Dokumententyp | Beschreibung |
|----------|---|--|
| A | Revisionsrelevante Dokumente | Sämtliche Dokumentation, welche im Zusammenhang mit der Revisionstätigkeit anfällt. |
| B | Nach Abschluss der Revision vernichten | Dokumentation, welche weder für einen lückenlosen Audit-Trail noch für zukünftige Revisionen benötigt wird: <ul style="list-style-type: none"> ■ spezifische Manuals oder Memos ■ handschriftliche Interviewnotizen, deren Informationen schon in die Revisionsakten eingeflossen sind usw. Diese Dokumente sind nach Abschluss der Revision zu vernichten (Shredder) bzw. zu löschen. |
| C | Nach Abschluss der Revision archivieren | Sämtliche Dokumente, welche für einen lückenlosen Audit-Trail benötigt werden, sowie alle anderen Dokumente mit relevanten Informationen für zukünftige Revisionen. |
| D | Nicht in Revisionsakten integriert | Dokumente, welche nicht für den Audit-Trail benötigt werden aber trotzdem für die Revision relevante Informationen enthalten. |
| E | In Revisionsakten integriert | Alle Dokumente, welche: <ul style="list-style-type: none"> ■ für Planung und Berichterstattung (Reporting) ■ für einen lückenlosen Audit-Trail benötigt werden. |
| F | Elektronische Dokumente | Elektronische Dokumente, welche im Laufe der Revision anfallen oder erstellt wurden, und eventuell für Nachfolgerevisionen von Interesse sein könnten und deshalb aufbewahrt werden. In diese Kategorie fallen zum Beispiel E-Mails. |
| G | Papierdokumente | Papierdokumente, welche im Laufe der Revision anfallen oder erstellt wurden, und die ev. für Nachfolgerevisionen von Interesse sein könnten und deshalb aufbewahrt werden. In diese Kategorie fallen zum Beispiel Manuals, Konzepte oder Organigramme. |
| H | Papierdokumente (Revisionsakten) | Alle zu den Revisionsakten gehörenden Papierdokumente. |
| I | Elektronische Dokumente (Revisionsakten) | Alle zu den Revisionsakten gehörenden elektronischen Dokumente. |
| J | Elektronisches Speichermedium (Serverlaufwerk des Kunden, Zip-Disk, MO oder CD-ROM) | Alle Dokumente aus Gruppe F. Die Speicherung auf dem elektronischen Speichermedium muss im Verzeichnis der jeweiligen Revision erfolgen. Nach Abschluss der Revision werden diese Dokumente dem Kunden, sofern sie nicht schon auf seiner Infrastruktur gespeichert sind, übergeben und bei der IT Audit Solution Group mit geeigneten Tools (Wipe Disk) gelöscht. |

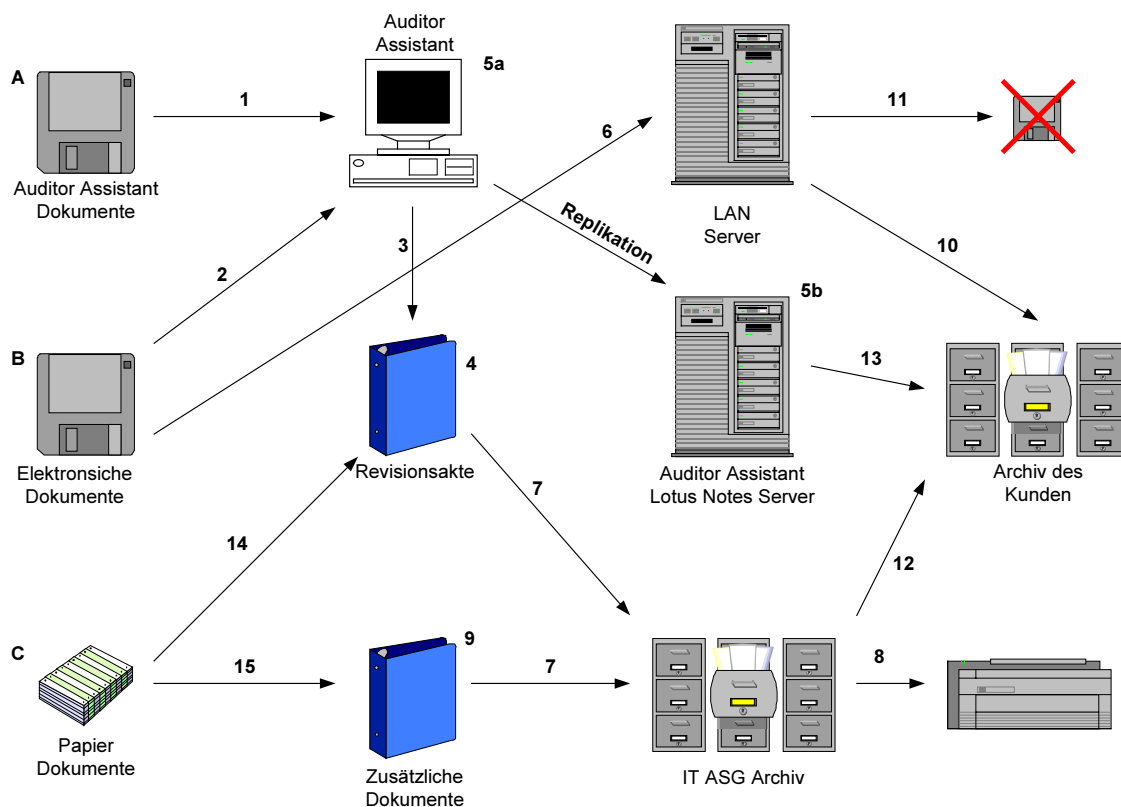
| | |
|--|---|
| K Archiv für Papierdokumente | Papier Dokumente, welche im Laufe der Revision anfallen oder erstellt wurden, und eventuell für Nachfolgerevisionen von Interesse sein könnten und deshalb aufbewahrt werden. Nach Abschluss der Revision werden diese Dokumente dem Kunden übergeben. |
| L Archiv Kunde | Permanentes Archiv der Internen Revision des Kunden. Enthält alle in Papierform vorliegenden Dokumente der Revisionsakten. Nach Abschluss der Revision werden diese Dokumente referenziert und indexiert dem Kunden übergeben. |
| M Auditor Assistant | Für jede Revision wird mit dem Tool Auditor Assistant eine elektronische Revisionsakte (Auditfile) erstellt. Welche das komplette Revisionsprogramm, alle Prüfschritte, Workpapers und Findings umfasst. Alle Dokumente aus Gruppe I (Elektronische Dokumente) werden ins AutoAudit-File integriert. Falls der Kunde auch Auditor Assistant benutzt, so kann ihm die Lotus Notes Datenbank, welche für die Revision erstellt wurde, übergeben werden. Sonst kann ihm ein PDF-File welches sämtliche, in Auditor Assistant enthaltenen, Dokumente enthält auf einem elektronischen Speichermedium übergeben werden. |

1.4.4. Vertraulichkeit der Dokumentation

Grundsätzlich sind sämtliche Revisionsakten als vertraulich einzustufen und im Sinne der entsprechenden internen Weisungen der IT ASG und des Kunden zu behandeln.

1.4.5. Detaillierte Darstellung des internen Dokumentenflusses

Die folgende Grafik zeigt im Detail den aktuellen internen Dokumentenfluss aller in die Revision involvierten Dokumente einschliesslich der Archivierung.



Legende zur Grafik

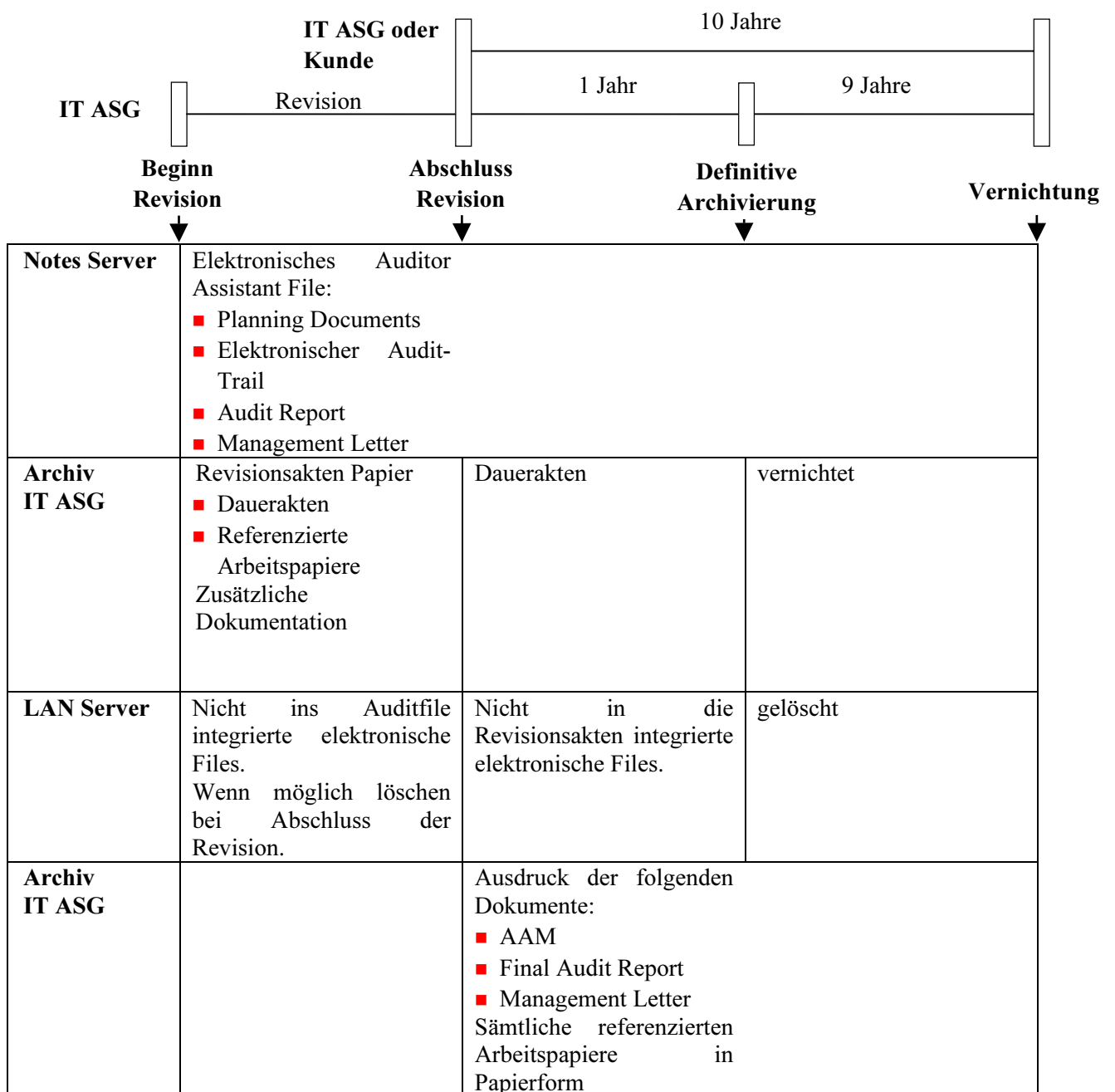
| # | Beschreibung |
|---|--|
| A | Direkt in Auditor Assistant erstellte Dokumente |
| B | Alle ausserhalb Auditor Assistant erstellten elektronischen Dokumente (Word, Excel, Powerpoint, HTML etc.) |
| C | Alle Papierdokumente |

-
- 1 Auditor Assistant Dokumente
Dokumente welche direkt im Auditor Assistant generiert werden (z. B. Workpaper, APAS, etc.).
-
- 2 Elektronische Dokumente
Falls sie für die Revision im engerem Sinne relevant sind, so sind sie direkt als Attachment im Auditor Assistant Workpaper zu integrieren
-
- 3 Dauerakten:
Nach Abschluss der Revision werden die Revisionsakten im Archiv abgelegt. Damit auch nach der Archivierung ein schneller Zugriff auf die wichtigsten Dokumente und Informationen einer Revision besteht, legt die IT Audit Solution Group pro Revision eine sogenannte Dauerakte an. Darin sind Kopien der folgenden Dokumente enthalten:
- Audit Planning Memorandum APM
 - Audit Announcement Memorandum AAM
 - Audit \ Report Status
 - Kickoff-Meeting Slides & Minutes
 - Audit Report (endgültige Version)
 - Management Letter (endgültige Version)
 - Wichtige Memos und E-Mails
 - Completion Statement
-
- 4 Revisionsakten Papier
Die Papier-Revisionsakten umfassen die Dauerakten (siehe Punkt 1) und alle Papierdokumente, welche als Evidence die im Management Letter genannten Schwachstellen belegen und somit in den Arbeitspapieren (Workpapers) referenziert sind.
-
- 5 Auditor Assistant File
Lokal Repliziertes (5a) sowie zentrales (5b) elektronisches Revisionsfile. Die lokale Lotus Notes Datenbank muss in regelmässigen abständen mit der zentralen Datenbank abgeglichen werden (Replikation). Umfasst folgende elektronisch vorhandenen Dokumente:
- Revisionsprogramm: RCMs und weitere Checklists
 - Audit-Trail: Workpapers, Finding Document und Evidence
 - Reporting: Audit Report sowie, Management Letter
- Falls der Kunde selbst Auditor Assistant einsetzt, wird das Revisionsfile dem Kunden übergeben. Alternativ dazu können sämtliche in Auditor Assistant enthaltenen Dokumente in ein oder mehrere PDF Files gedruckt werden und diese anschliessend auf eine CD-Rom gebrannt werden. Falls es der Kunde wünscht, wird die IT ASG danach alle elektronischen Informationen und Files mit einem geeigneten Tool löschen.
-
- 6 Zusätzliche Elektronische Dokumente
Elektronische Dokumente, welche nicht in die Revisionsakten integriert sind. Daher nicht relevant für Audit-Trail, werden auf dem LAN-Server im Verzeichnis der entsprechenden Revision gespeichert.
-
- 7 Revisionsakten Papier
Bis zum Abschluss der Revision werden die Papier Revisionsakten (siehe Punkt 2) durch das Revisionsteam in der eigenen Ablage aufbewahrt.
-
- 8 Zu vernichtende Papierdokumente
Zusätzliche Dokumente in Papierform (siehe Punkt 3), welche als Information für weitere
-

| | |
|----|--|
| | Revisionen im gleichen oder in anderen Bereichen nicht von Interesse sind, werden nach Abschluss der Revision vernichtet. |
| 9 | Zusätzliche Papierdokumente Alle Papierdokumente, welche nicht direkt als Evidence in die Revisionsakten integriert werden, welche während der Revision zusätzlich anfallen und als Hintergrundinformation dienen. |
| 10 | Audit Trail von referenzierten elektronischen Dokumenten Dem Kunden werden sämtliche, während der Revision angefallenen elektronischen Dokumente, welche Bestandteil des Audit Trails oder im engeren Sinne für die Revision relevant sind, für sein Archiv übergeben. |
| 11 | Zu löschende elektronische Dokumente Sämtliche auf dem LAN-Server gespeicherte elektronische Dokumente (siehe Punkt 4) sollten nach Abschluss der Revision, sofern es der Kunde wünscht, durch den Einsatz geeigneter Tools gelöscht werden. |
| 12 | Papier-Audit-Trail Dem Kunden werden sämtliche, während der Revision angefallenen Dokumente für sein Archiv übergeben. |
| 13 | Audior Assistant Datenbank Je nach Wunsch des Kunden können ihm entweder die Lotus Notes Workpaper Datenbank oder aber die darin enthaltenen Dokumente in PDF Format übergeben werden. |
| 14 | Referenzierte Arbeitspapiere In Papierform (siehe Punkt 2) |
| 15 | Zusätzliche Dokumente In Papierform (siehe Punkt 3) |

1.4.6. Zeithorizont der Aufbewahrung

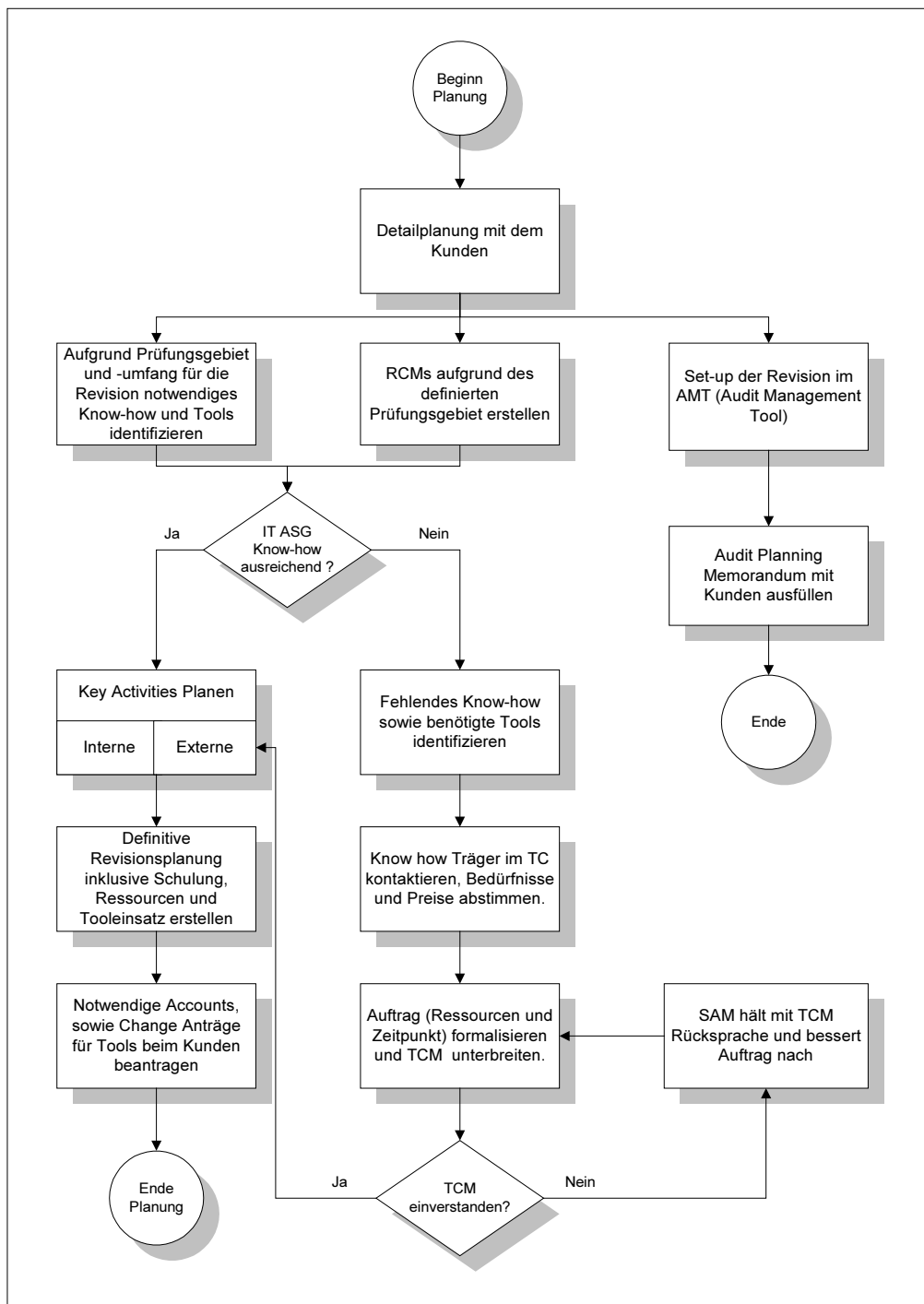
Falls es ein Kunde der IT Audit Solution Group wünscht, übernehmen wir auch die Archivierung aller mit der Revision in Zusammenhang stehenden Dokumentation nach dem folgenden Schema. Die Aufbewahrungspflicht von 10 Jahren ist gesetzlich vorgegeben.



2. Planung der Revision

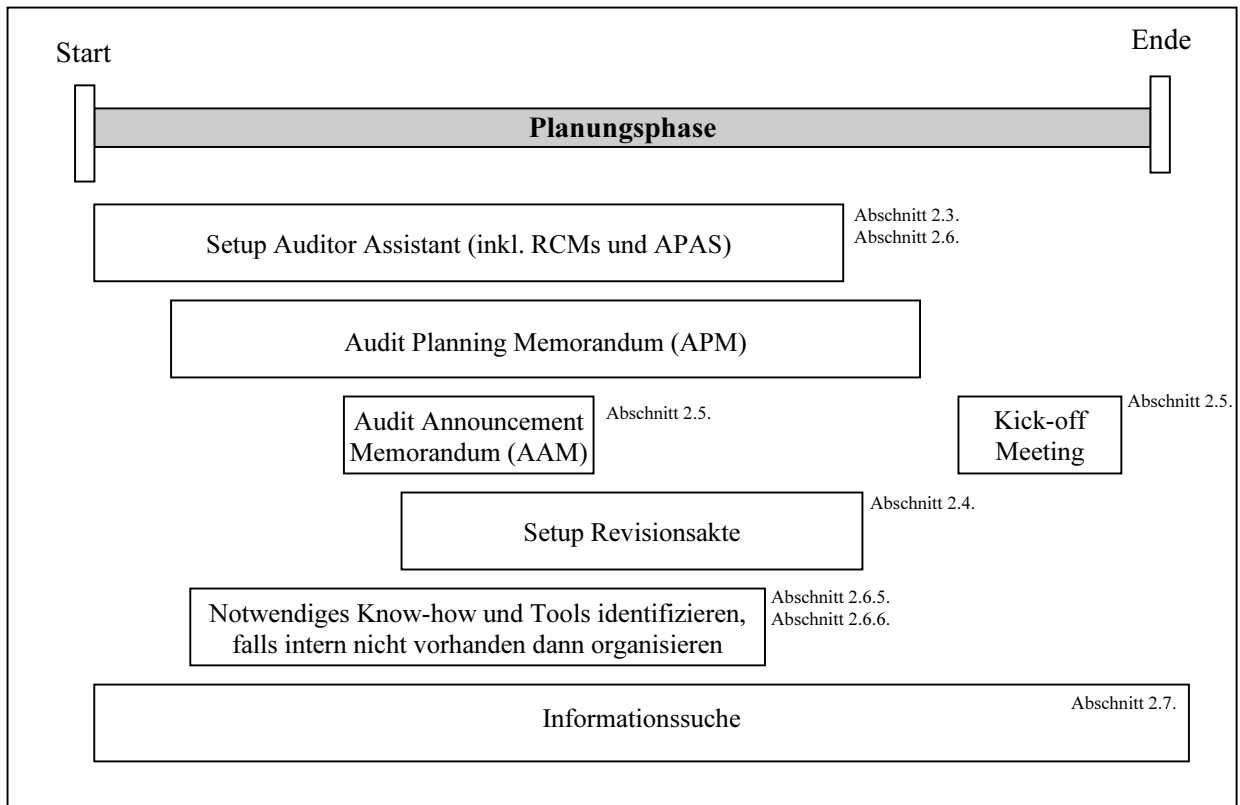
Der Audit Manager ist für den gesamten Planungsprozess verantwortlich. Eine Checkliste zu den Planungs- und Vorbereitungsaktivitäten befindet sich im Anhang.

2.1. Übersicht Planungsprozess



2.2. Übersicht der Planungsphasen

Folgende Grafik soll einen generellen Überblick über die Abfolge der verschiedenen parallelen Planungsaktivitäten geben. Die Phasenabfolge ist nicht streng nach Grafik zu verstehen, die Tätigkeiten können sich überlappen.



2.3. Set Up des Audits und des Audit Programms in Auditor Assistant

Auditor Assistant ist das von der IT Audit Solution Group eingesetzte elektronische Tool auf Basis von Lotus Notes zur Unterstützung des Revisionsprozesses und zur Dokumentation der Revisionsakten. Eine genauere Beschreibung über den Einsatz von Auditor Assistant befindet sich im Benutzerhandbuch.

2.3.1. Eröffnung einer Revision

Zweck:

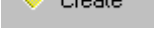
Um in Auditor Assistant eine Revision zu verwalten muss als erstes ein „Auditee“ eröffnet werden.

Beschreibung:

Der „Auditee“ wird in Auditor Assistant in der Management Datenbank über den Create Button (→ „Documents related to current document“ → „Auditee“ (Auswahl A)) erstellt. Eine detaillierte Anleitung über das Ausfüllen des Dokumentes befindet sich im Anhang.



2.3.2. Audit / Project / Activity / Summary (APAS) Dokument

Dieses Dokument wird in der Management Datenbank über den Create Button  erstellt. Dazu muss man den Auditee markieren für welchen man das APAS Dokument kreieren möchte, danach den Create Button drücken und im Fenster „Documents related to current document“ das APAS Dokument (Auswahl B) wählen.

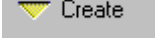
Das APAS Dokument dient dem Überblick über die Aufgabenverteilung innerhalb des Revisionsteams und den Status der Revision. Zudem besitzt es eine History-Funktion. Wichtig ist deshalb, das Dokument während der Revision laufend zu aktualisieren.

2.3.3. Audit Planning Memorandum (APM)

Zweck:

Das APM ist ein internes Dokument, welches als Teils der Dauerakten mit relevanten Background-Informationen zur Revision zu verstehen ist.

Beschreibung:

Das APM wird in Auditor Assistant in der Management Datenbank über den Create Button  erstellt (→ „Documents related to current document“ → „APM“ (Auswahl C)). Die Erstellung des APM fällt in den Verantwortungsbereich des Audit Managers. Ein Ausdruck des APMs ist im Ordner Dauerakten abzulegen. Eine detaillierte Anleitung über das Ausfüllen des Dokumentes befindet sich im Anhang.

2.4. Revisionsakte

Zweck:

Die Revisionsakte bildet zusammen mit den Informationen aus Auditor Assistant einen lückenlosen Audit Trail. Dieser sollte sich vom Set Up der Revision über das Fieldwork bis hin zum Reporting erstrecken und die Nachvollziehbarkeit aller wesentlichen Arbeitsschritte und –ergebnisse sicherstellen.

Beschreibung:

Im Revisionsordner sollten alle für die Revision relevanten Papierdokumente gesammelt werden. Nach Abschluss der Revision wird sie zusammen mit allen elektronischen Files dem Kunden abgegeben. Eine detaillierte Anleitung über das Führen der Akte befindet sich im Anhang.

2.5. Kontaktnahme mit revidierten Stellen

2.5.1. Audit Announcement Memorandum (AAM)

Zweck:

Das Audit Announcement Memorandum ist die offizielle Information an die revidierten Stellen über die Aufnahme einer Revision in ihrem Zuständigkeitsbereich.

Im AAM sind folgende Planungselemente enthalten: Start- und Endtermine, Prüfungsumfang (Audit Scope) sowie Angaben zum Revisionsteam.

Beschreibung:

Für das AAM ist die entsprechende Vorlage (Worddokument) zu verwenden.

Ein Beispiel zu einem AAM sowie zu einem E-Mail für den Versand des AAMs befindet sich im Anhang.

Ablage einer definitiven Version nach dem Versand:

- Das Worddokument muss als Attachment in das APAS Dokument, Feld „General Comments“ in der Management Datenbank von Auditor Assistant eingefügt werden.
- Ausdruck des Worddokumentes zur Ablage in die Dauerakten, Griff AAM.

Verteiler:

Es ist unbedingt auf einen vollständigen und korrekten Verteiler zu achten. Zum Verteiler gehören in jedem Fall:

- Leitung der betroffenen Ressorts
- Erste Stufe des Linien-Managements in den betroffenen Abteilungen
- Leitung Geschäftsbereich IT

Von Fall zu Fall sind weitere Hierarchie-Stufen oder betroffene Personenkreise in den Verteiler aufzunehmen.

2.5.2. Kick-off Meeting

Zweck:

- Vorstellung der IT Audit Solution Group
- Vorstellung der vertretenen internen Revision sowie des Revisionsteam
- Kurze Präsentation der geplanten Revision einschliesslich Vorgehen und Prüfungsumfang (Scope)
- Input revidierte Stelle (Auditees):
 - Bemerkungen zum Vorgehen/Prüfungsumfang
 - Definition von Ansprechpartnern
 - An Revisionsteam zu liefernde Dokumentation / Informationen

Vorgehen:

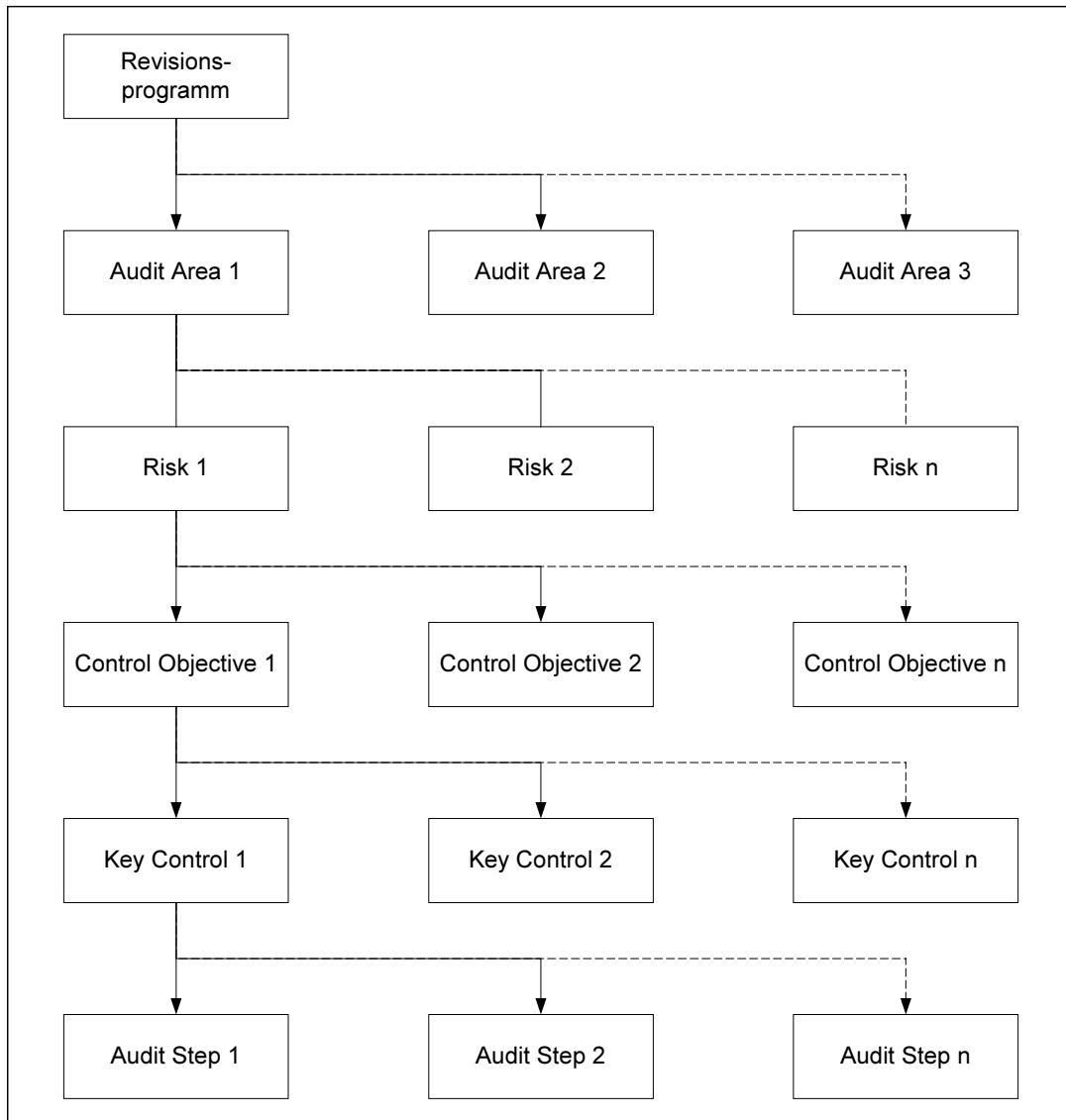
Ein Termin für das Kick-off Meeting ist nach oder gemeinsam mit dem Versand des AAMs zu organisieren.

Für das Meeting sind die Präsentations-Slides (Vorlagen vorhanden) anzupassen.

Ein Beispiel für eine Präsentation befindet sich im Anhang.

2.6. Revisionsprogramm

2.6.1. Aufbau eines Revisionsprogramms in Auditor Assistant



2.6.2. Übersicht der Struktur von Auditor Assistant

| Create | |
|--------|--|
| ▼ | Audit Group Zürich |
| ▼ | CIP Project Audit: 28.08.2000 |
| ▼ | A. Administration |
| ○ | MM Workpaper Index for: A. Administration |
| ▶ | 1. Planning |
| ▶ | 2. Reporting |
| ▶ | 3. Wrap-up |
| ▼ | B. Project Management |
| ○ | MM Workpaper Index for: B. Project Management |
| ○ | MM ▼ B.1 Risk: Die gewählte Lösung entspricht nicht der für das UBS Privat Banks optimalen Variante und führt somit zu Opportunitäts-, Zeit- und Geldverlusten. |
| ⚠ | MM ▼ B.1. Control: Sicherstellen, dass ein adäquater Business Case, eine abschliessende Kosten/Nutzen Analyse und einen Anforderungskatalog des Business vorliegen. |
| ⊕ | MM B.1.1 Test: Bedürfnisse des Business |
| ⚠ | MM B.1.2 Test: Machbarkeitsstudie |
| ⚠ | MM B.1.3 Test: Business Case |
| ○ | MM ▼ B.2 Risk: Durch die fehlende Sorgfalt fließen nicht alle Aspekte und/oder Bedürfnisse aller betroffenen Parteien in den Kaufentscheid ein. Dies kann sich durch Geld- und Zeitverluste, [missed opportunities] sowie fehlendem Herstellersupport manifestieren. |
| ⊕ | MM ▼ B.2. Control: Sicherstellen, dass die verfügbaren Lösungen sowie der Herstellersupport mit der gebotenen Sorgfalt evaluiert, und geprüft wurden. |
| ⊕ | MM B.2. Test: Evaluation der SW / Hersteller |
| ★ | MM ▼ B.3 Risk: Durch mangelnde Vertragsqualität wie zum Beispiel vertraglich nicht festgelegten Konventionstrafen oder das Fehlen wichtiger Zusätze kann die Betriebbarkeit der Applikation gefährdet werden und einen finanziellen Schaden entstehen. |
| ★ | MM ▼ B.3. Control: Die im Rahmen des Projektes abgeschlossenen Verträge sollten keine für die UBS nachteiligen Klauseln oder sonstige Zusätze enthalten. |
| ○ | MM B.3. Test: Verträge |
| ★ | MM ▼ B.4 Risk: Das fehlen von Business und/oder technischen Know-how könnte zu einem suboptimalen Ergebnis sowie zu Verzögerungen im Projektabschluss führen. |
| ⊕ | MM ▼ B.4. Control: Sicherstellen, dass die Aufbauorganisation des Projektes adäquat ist und sowohl das technische als auch das Business relevante Know-how umfasst. |
| ⚠ | MM B.4.1 Test: Aufbauorganisation |
| ○ | MM B.4.2 Test: Business User Involvement |
| ○ | MM B.4.3 Test: Respektieren von standards |
| ○ | MM ▼ B.5 Risk: Das fehlen einer adäquaten - Planung - Überwachung - Ressourcenzuweisung kann zu Verzögerungen und schliesslich |

Zur Zeit sind folgende Audit Areas definiert:

- IT Applications
- IT Security
- Firewall Audit
- IT Operations
- IT Projekt Management
- IT Management & Controlling
- IT Networks
- IT Change und Release Management
- IT Standards and Policies
- IT Disaster Recovery and Contingency Planning

Jede Audit Area setzt sich aus einer abstrakten, generell gültigen Schicht, welche Idealerweise aus Control Objectives und Key Controls besteht und einer auf die spezifisch auf die Technologie zugeschnittene Schicht (Audit Steps) zusammen. Die Summe der Audit Areas ergibt den Prüfungsumfang.

2.6.3. Prüfungsumfang (Scope) / Zeitbudget

Der Prüfungsumfang und das Zeitbudget (wird im APAS definiert) sind durch die vom Kunden genehmigte Offerte vorgegeben. Oft ist es nötig, aufgrund der Inputs aus dem Kick-off Meeting mit den revidierten Stellen den Prüfungsumfang der Revision im Hinblick auf die aktuelle Situation (z. B. Risikolage) anzupassen. Verantwortlich für die detaillierte Definition des Prüfungsumfanges ist, nach Rücksprache mit seinem Vorgesetzten (intern oder des Kunden), der Audit Manager.

2.6.4. Detailliertes Prüfprogramm (RCMs)

Zweck / Beschreibung:

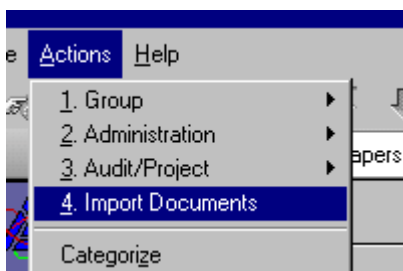
Das Prüfprogramm dient als konkrete Vorgabe für die Durchführung der Revision. Es setzt sich aus einer Anzahl von Kontrollzielen (Control Objectives) zusammen, deren Erfüllungsgrad durch die Revisionstätigkeit überprüft wird.

Die Auswahl von Kontrollzielen wird so getroffen, dass der vereinbarte Prüfungsumfang vollständig abgedeckt wird. Der vorgefundene Erfüllungsgrad der Kontrollziele lässt eine Aussage über die Qualität implementierter Kontrollen und damit auch über die Risikolage zu.

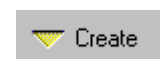
Eine Auswahl von Standard-Kontrollzielen steht in der Library von Auditor Assistant in Form von CobiT¹-Kontrollzielen zur Verfügung. CobiT gliedert die Informatik in Standardprozesse und definiert für jeden IT-Prozess Standard-Kontrollziele.

Für jedes Standard Control Objective welches ausgewählt wird gibt es in der Library von Auditor Assistant eine Anzahl von Key Controls sowie gegebenenfalls präzise Arbeitsanweisungen für den Revisor in Form von Audit Steps.

Vorgehen:



In der Workpaper Datenbank wählt man über das Menu Actions den Punkt Import Documents. Dort wählt man dann die Standard Workprogram Library aus. Danach kann man auswählen, ob man ganze Revisionsprogramme oder allenfalls nur einzelne Control Objectives importieren möchte. Zu guter letzt wählt man nun die relevanten Dokumente aus und importiert sie.



Ein individuelles Prüfprogramm kann auch erstellt werden. Über den Create Button muss als erster Schritt ein Risk Dokument erstellt werden. Falls man unter ein bestehendes Risk Dokument ein zusätzliches Control Objective hängen möchte, so kann man diesen Schritt weglassen und direkt ein Control Objective Dokument kreieren. Unter das Control Objective Dokument muss man danach noch ein Workpaper generieren. Wichtig ist, dass man bei der Generierung des jeweiligen Dokumentes immer das

¹ CobiT (Control Objectives for Information and related Technology), Framework der ISACA (Information Systems and Control Association)

Dokument wählt, unter welchem das zu kreierende Dokument zu liegen kommen sollte. Eine ausführliche Beschreibung findet sich im Auditor Assistant Handbuch.

2.6.5. Know-how und Tools

Je nach Revisionsthematik ist abzuklären ob die IT ASG in der Lage ist das notwendige Know-how für die Revision intern bereit zu stellen oder ob allenfalls externes Know-how aus den TCs notwendig ist. Sollte dies der Fall sein, dann ist mit den TCs im Detail abzuklären wer das Know-how hat und wer Ansprechperson ist. Der identifizierte Know-how Träger muss dann auch in die Ressourcenplanung mit einbezogen werden. In der Offerte sollten die Kosten des TC Mitarbeiters aufgeführt und beziffert sein (muss vorher mit dem TC ausgehandelt werden).

Weiter muss abgeklärt werden, ob die Tool Bibliothek der IT ASG alles Notwendige zur Verfügung stellen kann. Falls nicht, sind die notwendigen Schritte einzuleiten um sicherzustellen, dass die notwendigen Tools beim Anfang des Fieldworks zur Verfügung stehen.

Je nach Gegebenheiten sind weitere Vorbereitungsaktivitäten vorzunehmen, z. B.:

- Zugriffsberechtigungen für Systeme organisieren
- Zutrittsberechtigungen (Batches) für Räumlichkeiten organisieren
- Installationen von Analysetools
- ...

2.6.6. Revisionsprogramme und Tools des Kunden

Wünscht ein Kunde ausschliesslich den Einsatz seiner Revisionsprogramme (RCMs) und die Dokumentation der ausgeführten Prüfschritte entweder auf Papier oder sonst einem Tool, so ist es Aufgabe des Audit Managers die genauen Rahmenbedingungen vor dem Revisionsstart abzuklären und die Prüfprogramme des Kunden kritisch zu überprüfen und allenfalls, in Absprache mit dem Kunden zu ergänzen.

2.7. Informationssuche

Eine entscheidende Tätigkeit im Rahmen einer Revision ist die Beschaffung von Informationen. Es gilt, mögliche Informationsquellen zu identifizieren und aus den gefundenen Informationen die relevanten herauszufiltern.

Während der Planungsphase sind beispielsweise folgende **Informationstypen** in Betracht zu ziehen:

- Relevante Weisungen, Richtlinien und Standards
- Zu beachtende Gesetze und externe Regelungen
- Anwendbare Audit Standards und Prüfprogramme in Ergänzung zu CobiT
- IT-Umgebung: Hardware und Softwareumgebung
- Involvierte Business-Bereiche
- Involvierte Organisationseinheiten (Linie / Projekt) und deren Aufgabenbereiche
- Verantwortliche IT-Stellen

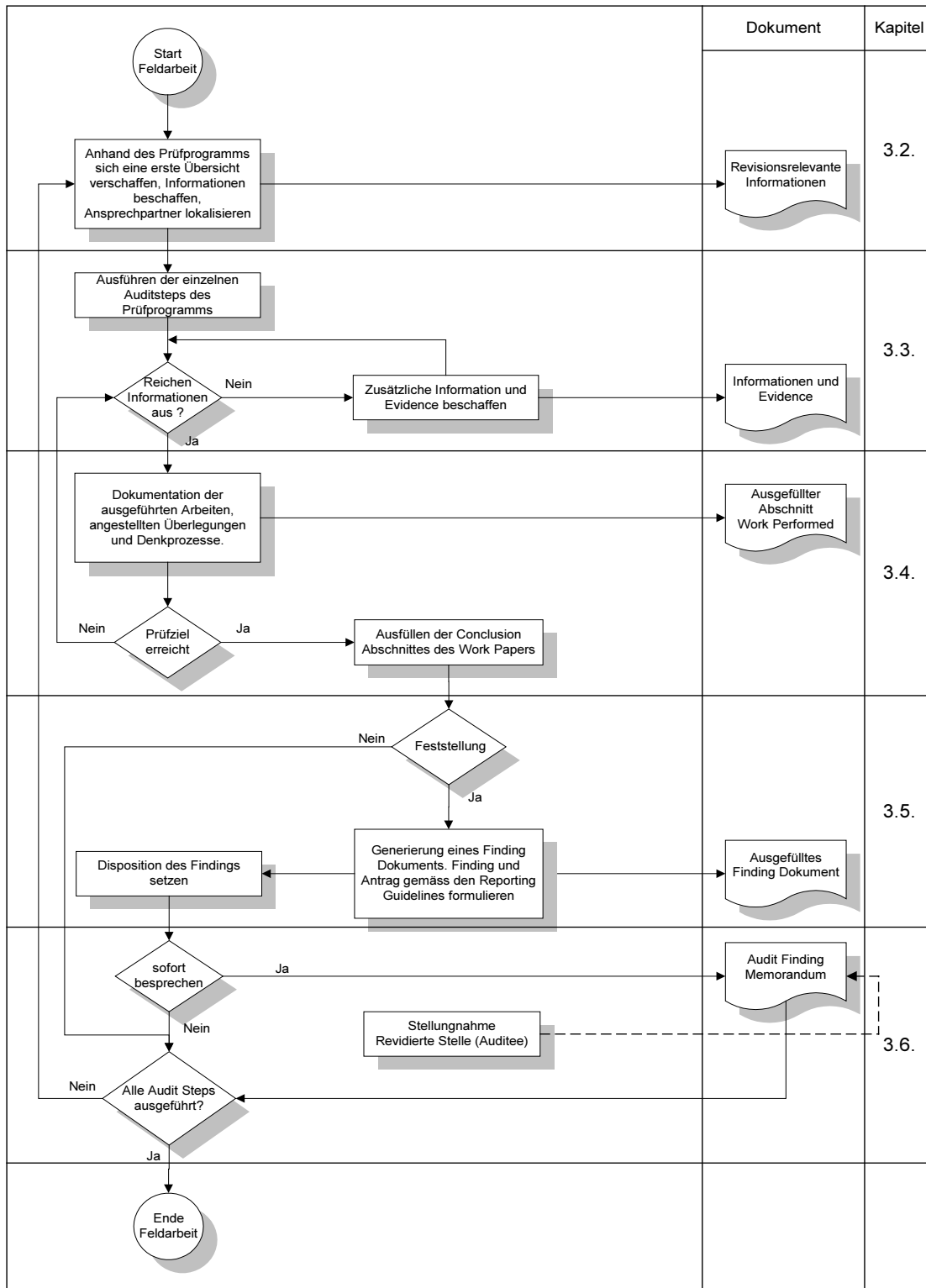


Als mögliche **Informationsquellen** sind zu nennen:

- Systranet (Besonders die IT ASG Homepage mit ihrer Linksammlung)
- WWW
- BS7799 Code of Practice
- ITSEC: IT Security Standards
- BSI-Grundschutz
- Specific Audit Checklists
- Dokumentationen zu früheren Revisionen
- ...

3. Field Work

3.1. Übersicht Prozessablauf Feldarbeit



3.2. Erste Informationsbeschaffung

Ziel:

Sich einen Überblick verschaffen und erste Informationen sammeln.

Vorgehen:

Das Vorgehen bei der Beschaffung der notwendigen Informationen bleibt dem einzelnen Auditor überlassen. Am effizientesten hat sich jedoch in der Praxis ein Top-Down Approach bewährt. Das heisst, dass man typischerweise mit den am Kick-off Meeting beteiligten Personen einen ersten Termin vereinbart damit:

- spezifische, individuelle Fragen zum Prüfprogramm oder Vorgehen beantwortet
- die notwendigen Massnahmen für den Einsatz von Tools bestimmt
- Dokumente zu den Prüfpunkten gesammelt
- weitere Ansprechpartner definiert

werden können.

Die im Laufe einer ersten Interview- und Informationssammelrunde angefallenen Informationen analysieren und, falls zu diesem Zeitpunkt schon möglich, den einzelnen Audit Steps zuordnen.

Resultat:

Sammlung von revisionsrelevante Informationen, welche einen ersten Überblick über die existierenden Prozesse, Schwachstellen, vorhandene Dokumente und weitere Ansprechpartner wiedergibt.

3.3. Ausführen der einzelnen Audit Steps

Ziel:

Es müssen in Menge und Qualität ausreichende Informationen gesammelt werden, damit zu den im Workpaper spezifizierten Kontrollzielen des Revisionsprogramms eine qualifizierte Beurteilung möglich ist.

Das heisst mit anderen Worten, dass sich Aussagen entweder:

- auf harten Fakten welche in Dokumenten enthalten sind, oder
- auf die Qualität eines für die Gesamtpopulation repräsentativen Querschnitts (Audit Sample) welche durch Compliance und Substantive Testings ermittelt worden ist,

stützen müssen.

Anhand der aus der ersten Informationsbeschaffung vorliegenden Informationen sollte man in der Lage sein, entweder

- zu dem Control Objective, welches durch Key Controls und Audit Steps geprüft werden sollte, anhand der vorliegenden Informationen eine abschliessende qualifizierende Aussage abgeben zu können, oder

- Anhaltspunkte und Ansprechpartner kennen, welche eine weitere, zielgerichtete, Informationsbeschaffung ermöglichen.

Zusätzlich muss die Informationssammlung die Anforderung erfüllen, dass alle im Revisionsbericht (Audit Report) gemachten Aussagen zu Schwachstellen und Risikolage durch entsprechende Beweisdokumentation (Evidence) belegt werden müssen.

Mündliche Aussagen und sogenannte Softfacts ohne entsprechende Evidence können zwar sehr nützliche Informationen zum Verständnis der Sachlage liefern, dürfen aber nicht die alleinige Grundlage für die Aussage über die Qualität eines Control Objectives sein.

Vorgehen:

Das Vorgehen sollte analog der ersten Informationsbeschaffung strukturiert sein:

- Informationsquellen bestimmen: Kontaktpersonen, Dokumentation
- Informationen sammeln: Interviews, Studium von Dokumentation, CAAT-Tools (Computer Aided Audit Tools)

Das Sammeln von Informationen erfolgt immer zielgerichtet und anhand des Revisionsprogramms (den im Workpaper definierten Audit Steps). Wichtig ist es, auf den Prüfungsumfang (Control Objectives und Key Controls) fokussiert zu bleiben. Stösst man auf Informationen, welche unerwartete Risikolagen anzeigen, kann es jedoch nötig sein den Prüfungsumfang entsprechend anzupassen.

Resultat:

Sammlung von Informationen, welche qualifizierte Aussagen zu den im Workpaper enthaltenen Key Controls bezüglich Schwachstellen und Risikolage zulassen. Schwächen müssen durch Belege (Evidence) bewiesen werden können.

3.4. Das Workpaper

3.4.1. Dokumentation der Feldarbeit

Ziel:

Die vorgenommenen Prüfungshandlungen, sowie die Aussagen zu den einzelnen im Workpaper enthaltenen Key Controls und somit über das übergeordnete Control Objectivs, inklusive Evidence, sind vollständig in den Revisionsakten zu dokumentieren (Audit-Trail).

Das „Weshalb“ man zu einem bestimmten Ergebnis gekommen ist, sollte mindestens stichwortartig dokumentiert sein und für einen aussenstehenden Dritten jederzeit, mit wenig Aufwand nachvollziehbar sein sowie adäquat mit referenzierter Evidence untermauert sein.

Vorgehen

Die Dokumentation der Revisionen erfolgt über die Applikation Auditor Assistant. Das für die Dokumentation sämtlicher Aktivitäten zentrale Dokument ist das Workpaper.

| <u>Work Paper</u> | |
|---|---|
| Audit Dept Division: Sweet Soles Sandle Company | |
| Audit Dept Group: Manufacturing | |
| Project Code: 12-1101-9051-00 | |
| Document Cross-References (Does not print) | |
| Hard-Copy Workpaper Reference (Does not print) | |
| Section: | B. Plant Operations |
| Workpaper Index: | B.1.1.1 |
| Test: | Review QC documentation and training procedures |
| Risk/Control Objective Information | |
| Key Controls | |
| Audit Steps | |
| 1. Identify and locate all documentation for Quality Control. | |
| 2. Verify copies are up to date (latest corporate revision) | |
| 3. Obtain training records for QC personnel | |
| 4. Verify they have completed update training on corporate required basis | |
| Work Performed | |
| Conclusion: | 6. Exception(s) noted—issue finding |
| Approvals | |
| Version History | |

Das Workpaper ist in sechs Bereiche unterteilt:

■ Risk / Control Information

In diesem Teil des Workpapers befinden sich die Informationen über das übergeordnete Risiko und das damit verbundene Control Objective. Diese Informationen sind zur Orientierung sehr nützlich, dies vor allem, falls der Sinn und Zweck der Key Controls und Audit Steps nicht ganz klar ist oder man sich verliert.

■ Key Controls

In diesem Abschnitt befinden sich die Key Controls, welche durch die Audit Steps verifiziert werden müssen.

■ Audit Steps

In der Sektion Audit Steps wird vorgeschrieben, welche Aktivitäten der Revisor auszuführen hat um die Key Controls zu validieren. Sie können je nach Prüfgebiet mehr oder weniger detailliert ausfallen. Sollte der Detaillierungsgrad Spielraum für eine persönliche Interpretation aufweisen, so wird erwartet, dass der

zuständige Revisor sich an den zu erfüllenden Key Controls und dem übergeordneten Control Objective orientiert. Es soll auf jeden Fall garantiert werden, dass die Key Controls adäquat überprüft wurden.

■ Work Performed

Hier muss der zuständige Revisor beschreiben, was er unternommen hat um die definierten Audit Steps auszuführen. Er sollte die ausgeführten Arbeiten, angestellte Denkprozesse und Überlegungen lückenlos dokumentieren. Die Work Performed Sektion sollte mindestens folgende Informationen enthalten:

- gelesene Dokumente
- geführte Interviews
- Systemoutputs
- bei Substantive und Compliance Testing, wie was womit getestet wurde
- Grösse des getesteten Samples sowie Ergebnisse des Tests
- Analyse, welche nachvollziehbar aufzeigt, wieso man zu der in der Conclusion angegebenen Bewertung der Key Controls gelangt

Der Denkprozess welcher zur Conclusion führt, sollte sich wie einen roter Faden durch diesen Abschnitt ziehen. Das Gütemass der Dokumentation sollte die Nachvollziehbarkeit der angestellten Überlegungen durch Dritte anhand der vorliegenden Sachlage und Evidence sein.

Evidence muss in dieser Sektion referenziert (Papier) oder direkt als Attachment (File) im Text eingefügt sein.

Resultat:

Sämtliche im Prüfprogramm enthaltene Workpaper sollten am Ende des Fieldworks ausgefüllt worden sein.

3.4.2. Beurteilung der Prüfungshandlung

Ziel:

Die gesammelten relevanten Informationen und Evidence werden den Prüfzielen (Key Controls und Audit Steps) zugeordnet. Es wird beurteilt, ob die Anforderungen der einzelnen Key Controls vollständig erfüllt sind oder ob mehr Informationen für eine gesicherte Aussage nötig sind. Es werden klare Aussagen bezüglich der Erfüllung der Key Controls, vorhandene Schwächen und den dadurch entstehenden Risiken gemacht.

Vorgehen:

- Analyse des Gaps zwischen SOLL (erwartete effektive Kontrollen) und IST (tatsächlich existierende Kontrollen)
- Beurteilung der Schwachstellen und der Risiken.

Resultat:

Für alle adressierten Control Objectives besteht eine klare und durch entsprechende Dokumente belegte Aussage über den Erfüllungsgrad, vorhandene Schwachstellen und die damit verbundenen Risiken.



3.4.3. Conclusion

Ziel:

Alle Workpaper haben am Ende der Revision einen Status welcher weder „Not yet Started“ noch „In Progress“ ist.

Vorgehen:

Alle Workpapers sind per Default auf „Not yet Started“ gesetzt. Beginnt nun ein Revisor das Workpaper beziehungsweise die darin enthaltenen Arbeitsanweisungen aktiv zu bearbeiten, so muss der Status auf „In Progress“ gesetzt werden.

Ist man schliesslich mit dem Bearbeiten der Audit Steps des Workpapers fertig, so ist je nach Ergebnis zu welchem man gelangt ist, der Radio Button für:

- Finished – No exceptions noted
- Exeption(s) noted – issue memo
- Exeption(s) notes – issue finding

anzuwählen.

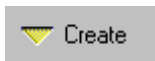
Werden die im Workpaper enthaltenen Audit Steps nicht ausgeführt, so muss die Option „Not Performed“ gewählt werden und nachvollziehbare Gründe dafür angegeben werden. Werden nicht alle Audit Steps ausgeführt so ist ebenfalls im Bereich „Work Performed“ ein Grund dafür zu nennen.

3.5. Das Finding Dokument

Ziel/Funktion:

Für alle relevanten Schwachstellen (Weaknesses) werden Feststellungen (Findings) erstellt. Die Findings dienen als Grundlage für den Management Letter (Sammlung aller relevanten Findings).

Vorgehen:

Über den Create Button  wird in Auditor Assistant ein Finding eröffnet. Ausgangspunkt für das Finding Document ist immer ein Workpaper.

Resultat:

Liste konsolidierter Findings:

- Für alle in den Management Letter oder Report aufzunehmenden Schwachstellen besteht ein als Management Letter, beziehungsweise bei schwerwiegenden Schwachstellen ein Report markiertes Finding Document.
- Für jedes Finding ist eine Beschreibung der Schwachstelle und des Risikos sowie eine Empfehlung zur Risikoreduktion vorhanden.
- Eine Stellungnahme des betroffenen Managements liegt vor und ist im Finding Document ausgewiesen.

3.5.1. Dokumentation des Findings und des Risikos

In diesem Abschnitt werden kurz allgemeine Anforderungen, welche an die Formulierung von Feststellungen und Empfehlungen sowohl im Management Letter als auch im Report gestellt werden, aufgelistet. Eine ausführlichere Beschreibung befindet sich in den separat erstellten Richtlinien zur Berichterstattung.

- Planung vor der Ausführung: sich immer verinnerlichen worüber man für wen was schreibt (Kundenorientierung und –sicht).
- Verzichte, wann immer möglich, auf umständliche Formulierungen.
- Vergewissere dich, dass deine Behauptungen faktisch korrekt sind. Bemühen dich, wo nötig, um entsprechende Unterlagen oder Stellungnahmen Dritter zur Absicherung der Aussagen.
- Konzentriere Dich auf Risiken und Wesentliches. Ist das Risiko gleich Null, besteht in der Regel kein Handlungsbedarf. Beschränke deinen Management Letter und Bericht ausschliesslich auf wesentliche Punkte.
- Sei exakt.
- Verdeutliche den Sachverhalt anhand von Beispielen (Fleisch am Knochen).
- Schweife nicht vom Thema ab. Beschränke dich auf das Wesentliche, ohne die Geprüften belehren zu wollen.
- Verwende stets eine einwandfreie Sprache, egal, ob es sich um Deutsch, Englisch oder Französisch handelt. Eine fehlerhafte Grammatik und schwache Satzkonstruktion hinterlassen einen unprofessionellen Eindruck.
- Hole nicht allzu weit aus, sondern halte dich strikt an die Materie.

- Identifiziere dich mit Ihren Aussagen, statt dich hinter Vorbehalten zu verstecken.
- Prüfe deine Berichte gewissenhaft. Verwende stets die “Rechtschreibprüfung”.
- Achte auf ein Professionelles Layout des Berichtes und des Management Letters.

3.5.2. Disposition der Findings

Erstellte Findings werden aufgrund ihrer Wichtigkeit und Dringlichkeit mittels einer Markierung im Dokument (Disposition) selber kategorisiert. Der Defaultwert ist „Pending Disposition“, das heisst, dass noch nicht entschieden wurde wie mit dem Finding weiter verfahren wird.

Optionen bei der Disposition:

| Keyword | Auswirkung |
|---------------------|--|
| Mitigating Controls | Es existiert zwar ein Risiko, jedoch sind ablauforganisatorische Massnahmen implementiert worden, welche erheblich verkleinern. Mitigating Controls im Feld Comments kurz beschreiben. |
| Not Significant | Im Nachhinein hat sich herausgestellt, dass der Sachverhalt nicht signifikant ist. Daher doch kein Finding. Gründe welche dazu führten im Feld Comments kurz beschreiben. |
| Verbal Discussion | Das Finding wurde dem relevanten Management mündlich mitgeteilt, da es sich nicht lohnte ein Memo zu verfassen. Im Feld Comments kurz beschreiben mit wem wann was genau diskutiert wurde. |
| Pending Disposition | Defaultwert |
| Report / ML / Memo | Im Feld „Select reporting methods“ auswählen ob das Finding in Form eines Memos, Management Letters oder Reports rapportiert werden soll. |
| Inaccurate | Im Nachhinein hat sich herausgestellt, dass der Sachverhalt nicht so ist. Daher doch kein Finding. Gründe welche dazu führten im Feld Comments kurz beschreiben. |
| Combined | Dieses Finding wurde mit einem weiteren kombiniert und wird nicht als eigenständiges Finding rapportiert. Im Feld Comments angeben, mit welchem Finding es kombiniert wurde. |

Es ist wichtig für den Erhalt eines kompletten Audit Trails zwischen Workpaper und Finding, dass ein Finding, welches sich im nachhinein durch neue Elemente oder bei der Schlussbesprechung nicht mehr als solches qualifizieren lässt, nicht gelöscht sondern anders kategorisiert wird.

Die Findings sollten gemäss den Report Writing Guidelines welche sich im Anhang befinden geschrieben werden.

3.6. Audit Finding Memorandum (AFM)

Funktion:

Kommunikation mit der revidierten Stelle (Auditee) während der Feldarbeit über vorgefundene Schwachstellen. Gegebenenfalls können so Korrekturmassnahmen sofort vorgenommen werden und Schwachstellen müssen nicht mehr im Management Letter oder Audit Report erwähnt werden bzw. das Finding entfällt nach einer Klarstellung durch den Auditee.

Beschreibung:

Das Erstellen eines AFMs wird durch Auditor Assistant zur Zeit nicht unterstützt. Sollte ein AFM erstellt werden so müssen die Feststellung und Recommendation mit cut & paste in das AFM Template eingefügt werden.

Die AFMs werden an die revidierte Einheit geschickt. Abhängig vom Ausmass des mit der Schwachstelle verbundenen Risikos ist abzuwägen, welche der folgenden Stellen ebenfalls orientiert werden:

- Direkter Vorgesetzter des Auditees
- Ressortleiter oder Gesamtprojektleiter (z. B. bei Grossprojekten)
- IT Risk Management

Achtung:

Ein AFM und ein als Memorandum markiertes Finding sind nicht zu verwechseln. Die diversen Kategorien von Findings (Report, ML, Memorandum) dienen intern dem Auditteam zur Priorisierung der Findings. Der Zweck der AFMs ist die Kommunikation mit dem Auditee. Alle Kategorien von Findings können als AFM markiert werden.

3.7. Der Review Prozess

Funktion:

Review-Notes dienen der Kommunikation für Fragen welche im Laufe der Revision über Dokumente oder Vorgehen entstehen können.

Beschreibung:

Review-Notes sind eigenständige Dokumente, welche durch Klicken auf den Create Button → Review Note aus einem beliebigen Dokument heraus erstellt werden. Sie sind in der View „All Docs w/ RNs“ sichtbar.

Reviewer macht seinen Kommentar im Review-Note Dokument und nicht direkt im betroffenen Dokument. Der Adressat der Review-Note seinerseits muss mit einer Review-Note Response (In der Review-Note Create Button → Review-Note Response).

Eine Review-Note kann nur vom Autor abschliessend geschlossen werden (Approved).

3.8. Der Approval Prozess

Zweck:

Sicherstellen, dass alle wichtigen Dokumente welche im Verlauf der Revision erstellt wurden von einer weiteren Person kontrolliert und genehmigt wurden.

Beschreibung:

Dokumente können nur von Personen mit Approval-Berechtigung (Rolle) genehmigt werden. Zuerst muss der Autor sein Dokument als Completed markieren (Approve Button → Completed).

Die für die weitere Genehmigung der Dokumente berechtigten Personen können das Dokument direkt öffnen, und den Approval Status je nachdem auf „In-charge“ oder „Senior“ setzen.

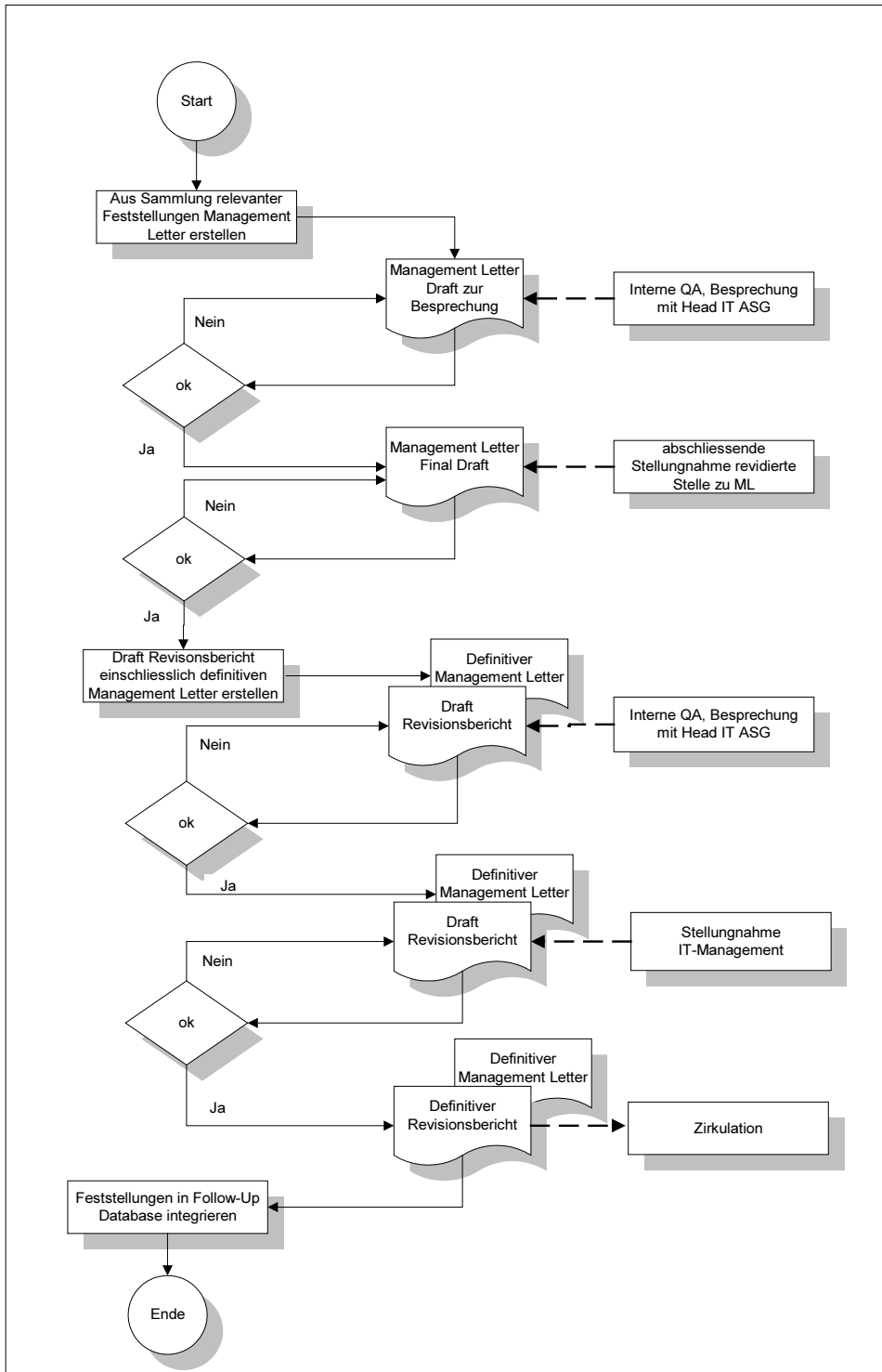
Nachdem Dokumente "approved" sind, können trotzdem noch Änderungen darin vorgenommen werden. Es ist aber zu beachten, dass die Dokumente dadurch den Status "approved" wieder verlieren und nochmals genehmigt werden müssen.

Bevor der Audit abgeschlossen werden kann, müssen folgende Dokumente "approved" sein:

- das APAS Dokument
- das APM
- alle Workpapers
- alle Findings

4. Reporting

4.1. Prozessübersicht



4.2. Der Management Letter

Zweck:

Im Management Letter hält die IT Audit Solution Group die während der Revision festgestellten Schwachstellen und Risiken fest und gibt Empfehlungen zum Minimieren dieser Risiken ab. Der Management Letter wird in einem ersten Schritt direkt an die revidierten Stellen und deren Linienmanagement gesandt. Diese geben zu den Feststellungen, Risikobeurteilungen und Empfehlungen der Revision eine Stellungnahme ab. Dadurch entsteht ein Dokument, welches die Ist-Situation, einschliesslich zu ergreifender Massnahmen und Termine, aus Sicht Revision und revidierter Stelle formal festhält.

Vorgehen:

Als Grundlage für den Management Letter dienen die sich während der Revision ergebenden Feststellungen (Findings). In den Management Letter fliessen alle als ML kategorisierten Findings ein.

Im Rahmen eines Closing Meetings sollte sich das IT ASG Revisionsteam und die revidierter Stelle versuchen, sich über die aufgeführten Punkte und Stellungnahmen zu einigen. Dabei geht es vor allem darum, auf beiden Seiten ein klares Verständnis der Aussagen zu erreichen und mögliche Missverständnisse zu bereinigen. Bis zur definitiven Version des Management Letters können deshalb auch mehrere Versionen erstellt und mit den betroffenen Stellen besprochen werden. Die verschiedenen Versionen müssen gemäss ihrem Status (z. B. Draft) und Version eindeutig gekennzeichnet sein.

Der Management Letter wird als Worddokument erstellt, ein Template liegt bereit. Genaue Instruktionen über dessen Anwendung befinden sich in den Report Writing Guidelines.

Struktur:

Der Management Letter besteht aus 3 Kolonnen:

- Feststellungen der IT ASG:
Zu jeder Feststellung wird zuerst eine kurze Beschreibung (ein bis zwei Sätze) der mit der Feststellung verbundenen Risikolage gemacht. Anschliessend folgt die Beschreibung des Ist-Zustandes, der die Risikolage verursacht. Im letzten Paragraph sollte die Risikolage genau spezifiziert werden.
- Anträge der IT ASG
In dieser Kolonne werden Anträge für Vorgehensweisen / Massnahmen zur Risikominderung/-beseitigung gemacht.
- Stellungnahmen/Massnahmen/Termine
Kolonne für das Feedback der revidierten Stelle

4.2.1. ML Draft for discussion

Dies ist die erste Version des Management Letters, welche an den Ansprechpartner der revidierte Stelle (z. B. Gruppen- oder Abt.-Leiter) kommuniziert wird. Falls mehrere Stellen involviert sind, ist es möglich an eine Stelle nur die jeweils relevanten Punkte zu schicken.

Inwiefern gleichzeitig eine Kopie zur Kenntnis an untenstehende Stellen geht, ist von Fall zu Fall abzuwägen und abhängig davon wie gesichert die Aussagen sind (Vorbereitung, Beweislage) bzw. von der jeweiligen Risikolage.

- Direkter Vorgesetzter
- Ressortleiter oder Gesamtprojektleiter (z. B. bei Grossprojekten)

Letzte Anpassung am Draft werden nach einer gemeinsamen Schlussbesprechung (Closing Meeting) mit der revidierten Stelle gegebenenfalls vorgenommen.

4.2.2. ML Final Draft

Diese Version des ML beinhaltet die Anpassungen an den Feststellungen und Empfehlungen der IT ASG aufgrund des Feedbacks der revidierten Stellen. Der ML Final Draft wird nun zur Stellungnahme an die revidierten Stellen verschickt.

Auch hier geht gleichzeitig eine Kopie zur Kenntnis an:

- Direkter Vorgesetzter
- Ressortleiter oder Gesamtprojektleiter (z. B. bei Grossprojekten)
- Leiter IT Risk Management
- Leiter Ressort Architecture & Business Support (IT Security)
- Auftraggeber

4.2.3. Definitiver Management Letter

Sobald alle Stellungnahmen der revidierten Stellen vollständig eingetroffen sind und sich die IT ASG damit einverstanden erklären kann, wird der definitive Management Letter erstellt.

Bei den Stellungnahmen ist unbedingt darauf zu achten, dass sie präzise sind und klare, terminierte Massnahmen einschliesslich verantwortlicher Person beinhalten.

Nicht zu vergessen: Die Stellungnahmen müssen in das Feld „Management Comments“ in Auditor Assistant kopiert werden.

4.3. Report

Zweck:

Der Revisionsbericht (Audit Report) ist das Endprodukt einer Revision. Er sollte dem Management in möglichst präziser, kurzer und verständlicher Form eine Übersicht über die Feststellungen geben, welche mit relevanten Risiken verbunden sind.

Risiken oder Feststellungen, welche sich während der Revision ergeben, die aber nicht zum eigentlichen Prüfungsumfang der Revision gehören, werden nicht in den Revisionsbericht aufgenommen. Die IT ASG informiert das betroffene Management mittels eines Memorandums.

Adressaten: Verwaltungsrat
Geschäftsleitung
Höheres Management (Leitung Geschäftsbereich)
Linienmanagement der revidierten Stellen (Stufe Ressortleitung)
Auftraggeber

Inhalt:

1. Zusammenfassung der Prüfungsergebnisse
 - Executive Summary
 - Zusammenfassung der Prüfungsergebnisse
 - Beurteilung über Zweckmässigkeit des internen Kontrollsystems
2. Tabelle Risikobeherrschung (Bewertung IT-Risk)
3. Wesentliche Feststellungen mit relevanten Risiken: Zusammenfassung der wichtigsten Punkte aus dem Management Letter.
4. Stellungnahmen von: Management / Präsidium

Vorgehen:

Als Grundlage zum Verfassen des Revisionsberichtes dient der Management Letter. Die Findings die als „Report“ in Auditor Assistant markiert sind, sind ja ein Subset der Findings welche in den Management Letter eingeflossen sind.

Nach der Erstellung der Quertabelle in Auditor Assistant werden die Feststellungen in das Report Template kopiert und anschliessend dort gemäss den Richtlinien zur Berichterstattung bearbeitet. Ein Beispiel eines Revisionsberichtes findet sich im Anhang.

4.4. Fristen der Berichterstattung

Im Interesse einer effizienten und zeitgerechten Arbeitsweise zur Erstellung des Revisionsberichtes wurde folgender Zeitrahmen festgesetzt, d. h. bis zu dieser Frist muss der Bericht zur Publikation weitergeleitet werden:

- Final Draft Management Letter: maximal eine Woche nach Abschluss des Fieldworks
- Final Draft Report: maximal 1 Wochen nach der Schlussbesprechung (nachdem der definitive Management Letter erstellt wurde)

4.5. Nummerierung der IT ASG Dokumente und Revisionen

| Dokument | Nr.-Struktur | Nr.-Vergabe durch |
|--|--|--------------------|
| Audit Nummer für Auditor Assistant | yy-nnn | Management Support |
| Revisionsbericht | ggyy-nnna Falls kein Mgmt Letter existiert, dann nur yygg-nnn | Management Support |
| Mgmt Letter | ggyy-nnnb falls kein Bericht existiert, dann nur yygg-nnn | Management Support |
| Memorandum (Minor findings, die in Zusammenhang mit der Revision stehen, aber im Mgmt Letter u. Bericht nicht vorkommen) | ggyy-nnnc | Management Support |
| Spezialberichte | Spezialnr. | Management Support |
| Stellungnahme / Opinion | ST-xxxxx | Management Support |

mit:

yy = Jahr (00 für 2000)

gg = IT ASG-Gruppe (noch näher zu definieren, im Moment nur IT verwenden)

nnn = Laufnummer

Bsp. **IT00-017**

4.6. Reporting nach den Reporting Standards des Kunden

Besitzt der Kunde eigene Templates und Reporting Standards so liegt es im Verantwortungsbereich des Audit Managers der betreffenden Revision sich über die Gepflogenheiten zu informieren und diese auch einzuhalten. Das gewünschte Reportingformat und der genaue Ablauf sollten Idealerweise am Ende der Planungsphase definiert sein, müssen aber auf jeden Fall vor dem Ende des Fieldworks feststehen.

5. Abschluss der Revision (Closing of Audit)

Nach dem Abschluss der Feldarbeit (Fieldwork) und dem Versand des definitiven Revisionsberichtes sind die Revisionsakten (in Auditor Assistant und in Papierform) sauber abzuschliessen und die Papierdokumente zu archivieren.

Auditor Assistant:

| | |
|---|---|
| Audit-Trail: | Ein vollständiger Audit-Trail aller elektronischen Dokumente muss vorhanden sein. Alle in Papierform vorhandenen Dokumente müssen auf den elektronischen Dokumenten in Audit referenziert werden. |
| Control Objectives: | Alle Objectives der RCM müssen ein Rating haben (vor dem Reporting). |
| Findings: | Alle Finding-Dokumente in Auditor Assistant müssen den Findings des definitiven Management Letters entsprechen (inkl. Stellungnahme des Managements). Gegebenenfalls sind die Dokumente in Auditor Assistant anzupassen. |
| Management Letter / Revisionsbericht | Die definitiven Versionen des Management Letters und des Berichtes sind in Auditor Assistant als Attachment zu integrieren. |
| Approval | Sämtliche Dokumente in Auditor Assistant müssen vom Audit Manager genehmigt werden. Nur dann kann der Audit abgeschlossen werden. |

Papier File:

| | |
|-----------------------|---|
| Workpapers | Alle Belege müssen vollständig und richtig referenziert werden. Anschliessend sind die Arbeitspapiere unter Angabe der Berichtsnummer in einer grauen Kartonschachtel zu archivieren oder dem Kunden abzugeben. |
| Dauerakte | Ausdruck des definitiven Management Letters und des Revisionsberichtes sind im Ordner Dauerakte abzulegen. Zusätzlich ist die Evidence List und das Audit Completion Statement zu drucken und in den Dauerakten abzulegen. |
| Zusätzliche Dokumente | Alle nicht als Evidence benötigte Dokumentationen, die auch nicht für weitere Revisionen von Interesse ist, sind zu vernichten. |
| LAN-Server | Alle nicht mehr benötigten Files sind zu löschen. |

6. Follow-up

Falls der Kunde es wünscht überprüft die IT ASG die von den revidierten Stellen im Management Letter definierten Massnahmen und Termine.

Für alle in den Revisionsbericht und Management Letter aufgenommenen Feststellungen besteht die Möglichkeit, diese in die Follow-up Datenbank von Auditor Assistant zu speichern. Dazu muss in den betreffenden Findings das Follow-up Kästchen angekreuzt werden.

Je nach Art und Umfang der gemachten Feststellungen sowie des bei periodischen Nachfragen angetroffenen Status der Umsetzung von angekündigten Massnahmen seitens der revidierten Stellen, können Nachfolgerevisionen in den gleichen Bereichen geplant und durchgeführt werden.

Damit eine Pendeuz definitiv als erledigt betrachtet werden kann, sollte mit der Meldung der Erledigung auch Audit Evidence“ geliefert werden, damit der Auditor sich selbst ein Bild der Lage verschaffen kann.

