

Richtlinien zur Berichterstattung

**Allgemein gültige Richtlinien der
IT ASG zur Berichterstattung**

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, 3. Januar 2001
©SYSTOR AG/Version 1.0

Inhaltsverzeichnis

Management Summary	4
1. Allgemeine Grundsätze	5
2. Aufbau der Revisionsberichte	6
2.1.1. Inhalt von Feststellungen	6
2.1.2. Aussagen zu Kontext/Wesentlichkeit	6
2.1.3. Aussagen zu Risiken	6
2.1.4. Zusatzinformationen zur Untermauerung von Feststellungen	6
2.2. Anträge	6
2.2.1. Inhalt von Anträgen	6
2.2.2. Umsetzbarkeit von Anträgen und Zeitpunkt der Implementierung	6
2.3. Stellungnahme seitens des Managements	7
2.3.1. Genehmigung/Ablehnung durch das Management	7
2.3.2. Bezieht sich die Stellungnahme auf die Feststellung und den Antrag?	7
2.3.3. Verantwortlichkeit für die Lösung des Problems	7
2.3.4. Frist für die Implementierung von Korrekturmaßnahmen	7
2.4. Siehe separates Kapitel "Audit Ratings"	7
2.5. Standardabkürzungen und Verwendung von Akronymen	9
3. Struktur der Revisionsberichte	10
3.1. Revisionsberichte	10
3.1.1. Zweck	10
3.1.2. Form und Inhalt	10
3.1.3. Deckblatt/Verteiler	10
3.1.4. Schlüsselinformationen zur Revision (Bericht Seite 2)	11
3.1.5. Hintergrundinformationen	11
3.1.6. Prüfungsumfang	11
3.1.7. Zusammenfassung der Prüfungsergebnisse	11
3.1.8. Zweckmäßigkeit des internen Kontrollsystems	12
3.1.9. Nicht behobene Mängel der letzten Revision	12
3.1.10. Risikobeherrschung	12
3.1.11. Wesentliche Feststellungen	13
3.1.12. Stellungnahme: Direktion	13
3.1.13. Stellungnahme: Geschäftsleitung	13
3.1.14. Stellungnahme: Konzernleitung	14
3.1.15. Stellungnahme: Präsidium	14
3.2. Management Letters	14
3.2.1. Zweck	14



3.2.2. Form und Inhalt	14
3.3. Memoranden	14



Management Summary

Während oder im Anschluss an eine Revision werden abschliessend Revisionsberichte, Management Letters und Revisionsmemoranden erstellt. Diese schriftlichen Mitteilungen stellen den regelmässigen Kommunikationsaustausch zwischen den beteiligten Parteien wie den Mitglieder des Verwaltungsrates, Führungsgremien des Unternehmens und der IT ASG der SYSTOR AG. Folglich ist es von zentraler Bedeutung, dass sämtliche schriftliche Mitteilungen seitens der IT ASG sowohl inhaltlich als auch optisch höchsten Ansprüchen genügen.

Der Hauptzweck der vorliegenden Richtlinien ist dementsprechend die Unterstützung der Mitarbeiter bei der Erstellung von Revisionsberichten, Management Letters und Revisionsmemoranden, damit diese einen logischen Aufbau aufweisen, in Stil und Layout einheitlich und sauber strukturiert sind.



1. Allgemeine Grundsätze

In den folgenden Abschnitten werden die einzelnen Richtlinien zur Unterstützung der Revisoren bei der Erstellung von Revisionsberichten, Management Letters und Revisionsmemoranden ausführlich beschrieben. Dabei gelten insbesondere auch die folgenden allgemeinen Grundsätze:

- Planung vor Ausführung: bedenke zuerst worüber du wem schreiben willst.
- Verzichte, wann immer möglich, auf umständliche Formulierungen.

Vergewissere dich, dass deine Behauptungen faktisch korrekt sind. Bemühe dich, wo nötig, um entsprechende Unterlagen oder Stellungnahmen Dritter zur Absicherung deiner Aussagen.

Konzentriere dich auf Risiken und Wesentliches. Ist das Risiko gleich Null, besteht in der Regel kein Handlungsbedarf. Beschränke deinen Revisionsbericht ausschliesslich auf wesentliche Punkte:

- Sei exakt.
- Verdeutliche den Sachverhalt anhand von Beispielen.
- 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 Englisch, Deutsch Italienisch 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 deinen Aussagen, statt dich hinter Vorbehalten zu verstecken.
- Prüfe deine Berichte gewissenhaft. Verwende stets die "Rechtschreibprüfung".



2. Aufbau der Revisionsberichte (Bericht und Management Letter)

2.1. Feststellung

2.1.1. Inhalt von Feststellungen

Richtig

Feststellungen müssen faktisch korrekt sein. Ihre Korrektheit muss aus den Arbeitspapieren nachweisbar sein. Immer zuerst die Feststellung ausführen.

Falsch

Der Bericht darf keine Gerüchte enthalten. Halte dich ausschliesslich an Fakten und im Rahmen Ihrer Aufgabe erbrachte Beweise (sogenannte Audit Evidence). Verzichte auf allgemeine Formulierungen. Beschränke dich auf die Materie. Verzichte darauf, Meinungen im Rahmen von Feststellungen zu rapportieren.

2.1.2. Aussagen zu Kontext/Wesentlichkeit

Zur Klärung des Sachverhalts kann es unter Umständen erforderlich sein, einer Feststellung eine Aussage zum näheren Kontext und/oder der Wesentlichkeit der Feststellung anzufügen.

2.1.3. Aussagen zu Risiken

Das Risiko in Bezug auf eine Feststellung sollte für alle Leserinnen und Leser des Revisionsberichts klar ersichtlich sein. Unmittelbar nach der eigentlichen Feststellung auf das vorliegende Risiko eingegangen werden. Sind mehrere Risiken involviert, ist das jeweils wichtigste in den Bericht aufzunehmen. Der Management Letter hingegen sollte alle enthalten.

2.1.4. Zusatzinformationen zur Untermauerung von Feststellungen

Für ein besseres Verständnis einer Feststellung kann es unter Umständen erforderlich sein, ein paar Zusatzangaben zu machen. Diese sind nach der knappen Erklärung der Feststellung anzubringen. Fasse dich möglichst kurz.

2.2. Anträge

2.2.1. Inhalt von Anträgen

Anträge sollten sich strikt auf den Sachverhalt beziehen. Anträge müssen klar und eindeutig formuliert werden.

2.2.2. Umsetzbarkeit von Anträgen und Zeitpunkt der Implementierung

Anträge müssen umsetzbar sein. Lässt sich ein Antrag nicht kurzfristig umsetzen, sind zu Kompensationszwecken, sofern möglich, provisorische Kontrollmechanismen zu empfehlen. Es sollten nur Anträge verabschiedet werden, deren Umsetzbarkeit ausser Frage steht. Es ist darauf zu achten, dass nicht der Eindruck entsteht, der eine oder andere Antrag sei weniger dringlich.



2.3. Stellungnahme seitens des Managements

2.3.1. Genehmigung/Ablehnung durch das Management

Das Management sollte in seiner Antwort Stellung dazu nehmen, ob es eine Feststellung und Anträge genehmigt oder ablehnt. Es darf keine Meinungsverschiedenheit in bezug auf Fakten bestehen.

Nur in Ausnahmefällen wird eine Ablehnung durch das Management im Management Letter vermerkt. Dies ist zum Beispiel dann der Fall, wenn eine grundsätzliche Meinungsverschiedenheit herrscht. Gegebenenfalls hat die IT ASG in einer Notiz auf die näheren Gründe einzugehen, weshalb an einem bestimmten Antrag festzuhalten sei.

2.3.2. Bezieht sich die Stellungnahme auf die Feststellung und den Antrag?

Bevor eine Stellungnahme seitens des Managements in den definitiven Management Letter und Revisionsbericht aufgenommen wird, muss geprüft werden, ob sie sich tatsächlich auf die fragliche Feststellung bezieht. Sollte eine Stellungnahme nicht unmittelbar auf die Feststellung eingehen, kann dies zwei Gründe haben: Entweder wurde die Tragweite des Sachverhalts seitens des Managements nicht vollumfänglich erkannt, oder Letzteres zog es vor, nicht direkt auf das eigentliche Thema einzugehen.

2.3.3. Verantwortlichkeit für die Lösung des Problems

Die für die Problemlösung im Rahmen der einzelnen Feststellungen verantwortliche Person ist im Management Letter namentlich mit Angabe der Abteilung am Schluss der Stellungnahme aufzuführen.

2.3.4. Frist für die Implementierung von Korrekturmaßnahmen

Falls das Management bereits Korrekturmaßnahmen eingeleitet hat, sollte es dazu aufgefordert werden, in seiner Stellungnahme darauf hinzuweisen. Stellungnahmen müssen jeweils ein Umsetzungstermin (Datum) beinhalten. Diese Frist muss für die IT ASG oder die jeweilige Konzernrevision annehmbar sein.

2.4. Siehe separates Kapitel "Audit Ratings"

Die Revisionsberichte der IT ASG beinhalten ein Audit Rating. Das Audit Rating soll das Management des revidierten Unternehmens bei der Bewertung der Qualität der Kontrollmechanismen und bei der Beurteilung der potentiellen Risiken innerhalb der jeweiligen Verantwortungsbereiche unterstützen.

Das Audit Rating wird durch eine Reihe von Faktoren bestimmt, einschliesslich:

- **Bedeutung / Wesentlichkeit der Feststellungen**
Es werden nur wesentliche Feststellungen im definitiven Revisionsbericht aufgeführt. Einzelne Feststellungen werden schwerwiegender sein als andere. In dieser Hinsicht muss der Aspekt der Wesentlichkeit oder des Verlustrisikos sorgfältig erwogen werden. Auch Feststellungen betreffend die Gefahr eines Imageverlusts, mögliche Sanktionen seitens der Aufsichtsbehörden und Betriebsunterbrechung können wesentlich sein.
- **Anzahl der Feststellungen**
Die Anzahl der rapportierten Feststellungen an sich bestimmt noch nicht das Audit Rating. So ist es möglich, dass eine Feststellung so schwerwiegend ist, dass sie ein schlechtes Audit Rating bewirkt.



Andererseits kann eine Reihe von Feststellungen, die einzeln gewertet als nicht wesentlich betrachtet würden, zusammengenommen auf bedeutende Mängel im Kontrollumfeld hinweisen. Die kombinierten Auswirkungen aller Feststellungen auf das interne Kontrollsystem müssen bei der Festsetzung des Audit Ratings berücksichtigt werden.

■ **Wiederholt auftretende Feststellungen**

Früher rapportierte Feststellungen, bei denen keine Abhilfe geschaffen wurde, lassen das aktuelle Rating normalerweise schlechter ausfallen als beim ursprünglichen Revisionsbericht. Die ursprüngliche Feststellung war bereits bedeutend: die Untätigkeit der Führung diesen Sachverhalt zu lösen ist für sich genommen auch ein wesentlicher Mangel; dazu nimmt das Verlustrisiko zu, je länger die Schwachstelle offen bleibt.

Die Höhe des eingegangenen Risikos, das aus einer bedeutenden Feststellung hervorgeht, muss bei der Bestimmung des Audit Ratings stets berücksichtigt werden. Die nachfolgenden Beispiele sind als schwerwiegendere Fälle einzustufen:

- Gravierende Mängel im Kontrollumfeld eines Hauptsystems oder -prozesses, die zu einem Missbrauch oder Verlust von Vermögenswerten führen könnten.
- Bedeutende Abweichung von der Geschäftspolitik des Unternehmens.
- Bedeutende Abweichung von den Vorschriften der Aufsichtsbehörden.
- Bedeutendes Risiko einer Betriebsunterbrechung infolge von Schwachstellen im operativen Bereich.
- Wesentliche Fehler in der Finanzberichterstattung, die vom Management bisher nicht erkannt wurden.
- Bisher nicht gemeldeter Betrug oder Diebstahl.

Audit Ratings sind nicht als Ausweis für persönliche Leistungen gedacht, da sie nicht immer von Einzelpersonen abhängen. Oft haben andere Organisationseinheiten und Aktivitäten Einfluss auf die durch die Revision geprüften Prozesse und Funktionen und können damit ein schlechteres Rating beeinflussen.

Die IT ASG unterscheidet die folgenden Audit Ratings:

■ **Gut (good):**

Das interne Kontrollsystem ist wirksam. Die Prüfung gab zu keinen wesentlichen Bemerkungen im Revisionsbericht Anlass. Ein Audit Rating «gut» sagt aus, dass im geprüften Bereich angemessene und wirksame Kontrollmechanismen bestehen und dass die Geschäftspraktiken mit den Gesetzen, Vorschriften sowie den festgelegten Abläufen und der Geschäftspolitik im Einklang stehen.

■ **Zufriedenstellend (satisfactory):**

Die interne Kontrolle ist mit wenigen Ausnahmen wirksam. Ein Audit Rating «zufriedenstellend» sagt aus, dass im geprüften Bereich angemessene und wirksame Kontrollmechanismen bestehen und dass die Geschäftspraktiken im Allgemeinen mit den Gesetzen, Vorschriften sowie den festgelegten Abläufen und der Geschäftspolitik im Einklang stehen.

■ **Mit Vorbehalt (qualified):**



Schwachstellen im internen Kontrollsystem. Die Mängel sind zu beheben. Ein Audit Rating «mit Vorbehalt» sagt aus, dass ein oder mehrere grundlegende Kontrollmechanismen fehlen oder unwirksam sind, was potentiell zu einer unbefriedigenden Situation führen kann, falls nicht innert nützlicher Frist Abhilfe geschaffen wird. Bei den Geschäftspraktiken wurden Mängel festgestellt.

■ **Ungenügend (unsatisfactory):**

Wesentliche Mängel, die sich nachhaltig auf die Risikolage des geprüften Unternehmens (Verluste/Verlustpotential, Image-Risiko, regulatorische Sanktionen, Betriebs-/Systemunterbruch-Risiko) auswirken oder auswirken können. Nicht behobene, wesentliche Mängel seit der letzten Revision. Es besteht ein unverzüglicher Handlungsbedarf. Ein Audit Rating «ungenügend» sagt aus, dass die Kontrollmechanismen innerhalb der Organisation nicht angemessen sind oder die Geschäftspraktiken nicht mit den Gesetzen, Vorschriften sowie den festgelegten Abläufen und der Geschäftspolitik im Einklang stehen. Der definitive Revisionsbericht wird Anträge oder kritische Feststellungen zu Schlüsselbereichen enthalten.

Sofortige Auswirkung der Audit Ratings:

Sobald die Revision abgeschlossen ist, werden in der Regel das Management des Unternehmensbereichs sowie alle Mitglieder der Konzernleitung über potentielle ungenügende Revisionsresultate informiert, indem ihnen ein Vorab-Info-Exemplar des Revisionsberichtsentswurfs zugestellt wird.

2.5. Standardabkürzungen und Verwendung von Akronymen

Für die Verwendung von Abkürzungen und Akronymen gelten folgende allgemeine Regeln:

In einem Revisionsbericht oder Management Letter verwendete Akronyme sind bei ihrer ersten Verwendung im Text vollständig zu erklären. Beispiel: ABS («Association of Banks in Singapore»; Bankvereinigung in Singapur). Hingegen kann auf eine Erklärung von «Industrienormen» wie zum Beispiel Swift oder Cedel verzichtet werden.

Für sämtliche Währungen ist die jeweilige ISO-Norm (International Organization for Standardization) zu verwenden.

3. Struktur der Revisionsberichte

3.1. Revisionsberichte

3.1.1. Zweck

Revisionsberichte sollen dem Management und den Mitgliedern des Verwaltungsrates einen Überblick über die Ergebnisse und Hauptbelange der einzelnen Revisionen vermitteln.

3.1.2. Form und Inhalt

Für die Darstellung von Revisionsberichten ist ein verbindliches Layout vorgegeben welches, sofern vom Kunden nicht anders gewünscht, zum Einsatz kommt. Desgleichen ist die Struktur von Revisionsberichten klar vorgegeben. Er umfasst die folgenden Standardabschnitte:

- Deckblatt/Verteiler
- Hintergrundinformationen
- Prüfungsumfang
- Zusammenfassung der Prüfungsergebnisse
- Zweckmässigkeit des internen Kontrollsystems
- Nicht behobene Mängel der letzten Revision
- Risikobeherrschung
- Wesentliche Feststellungen
- Stellungnahme: zuständiges Management
- Stellungnahme: Geschäftsleitung
- Stellungnahme: Konzernleitung (falls nicht mit Geschäftsleitung identisch)
- Stellungnahme: Präsidium oder Verwaltungsrat
- Angaben über die geprüfte Geschäftstätigkeit (optional)

Weitere Angaben zum Inhalt dieser Standardabschnitte finden Sie in den nachfolgenden Kapiteln.

3.1.3. Deckblatt/Verteiler

Diese Seite umfasst die folgenden Angaben: Berichtsnummer und -datum, Name der Einheit und Revisionsinhalt, Audit Rating, Verteiler mit den Mitgliedern des Senior Managements, an die der Bericht im Original geht, sowie Verteiler für Kopien des Berichts, Unterschrift des Verantwortlichen der IT ASG sowie des Verantwortlichen der zuständigen Revisionseinheit.

3.1.4. Schlüsselinformationen zur Revision (Bericht Seite 2)

Diese Seite umfasst die folgenden Angaben: Revisionsbezeichnung, Revisionsperiode (d. h. Zeitraum, während dem die Revision durchgeführt wurde), Aufzeichnungen zu Diskussionen mit dem lokalen Management des Unternehmensbereichs und dem regionalen Management betreffend die Revisionsergebnisse, Aufzeichnungen zu Diskussionen mit dem Senior Management des Unternehmensbereichs betreffend den Berichtsentwurf, Name(n) des/r verantwortlichen Auditors/-en sowie der Manager der IT ASG.

Des weiteren enthält diese Seite Hintergrundinformationen sowie Angaben zum Prüfungsumfang, wie im Folgenden erläutert.

3.1.5. Hintergrundinformationen

In den ersten Abschnitt gehört eine kurze Erläuterung, um die Revision in den spezifischen Kontext zu stellen. Schlüsselinformationen und Kennzahlen gehören in einen Anhang zum Bericht. Sie umfassen unter anderem die bisherige Unternehmensgeschichte, aktuelle Neuerungen, Entwicklungspläne sowie Transaktionsvolumen.

3.1.6. Prüfungsumfang

Der Prüfungsumfang beinhaltet folgendes:

Unter «Prüfungsumfang» versteht man eine knappe Erläuterung der übergeordneten Prüfungsziele, an denen sich eine einzelne Revision orientieren sollte. Der Prüfungsumfang sollte sich prinzipiell an der in der Offerte gemachten Angaben orientieren.

Die übergeordneten Prüfungsziele lassen sich in spezifische Einzelziele unterteilen, die jedoch nur im Anhang zum Management Letter zu erwähnen sind. Ebenso sind Detailangaben zu den durchgeführten Kontrollen, wie zum Beispiel die Anzahl geprüfter Posten, im Rahmen des Prüfungsumfangs dem Management Letter beizufügen.

Falls ein zentrales Element in der Revision unberücksichtigt bleiben soll, ist dies unter Angabe von entsprechenden Gründen festzuhalten.

- Der Prüfungsumfang sollte sich auf Seite 2 des Berichts beschränken.
- Der Prüfungsumfang sollte kurz und bündig ausfallen.
- Der Prüfungsumfang sollte möglichst konkret formuliert werden.
- Der Prüfungsumfang soll allgemeinsprachlich formuliert werden, damit er auch von Dritten, die mit dem Unternehmenskontext nicht vertraut sind, verstanden wird.

3.1.7. Zusammenfassung der Prüfungsergebnisse

Um das Senior Management auf bestimmte Schlüsselbereiche aufmerksam zu machen und/oder ein «abgerundetes Bild» der im Rahmen der Revision zu prüfenden Situation respektive des zu prüfenden Bereichs zu vermitteln, kann am Anfang des Paragraphs ein kurzer Abschnitt hinzugefügt werden. Von



dieser Möglichkeit ist allerdings nur Gebrauch zu machen, wenn ein «ungenügendes» Rating oder ein solches «mit Vorbehalt» vorliegt.

Sind bei einer vorhergehenden Revision festgestellte wesentliche Probleme in der Zwischenzeit bereinigt worden, ist an dieser Stelle ein entsprechender Vermerk zu machen.

3.1.8. Zweckmässigkeit des internen Kontrollsystems

Es ist Aufgabe der IT ASG, ein Gesamturteil zur Wirksamkeit des internen Kontrollsystems im Geprüften Bereich abzugeben. Dabei ist darauf zu achten, dass die Schlussfolgerungen klar und frei von jeglichen Widersprüchen formuliert werden.

Es ist unbedingt darauf zu achten, dass an dieser Stelle nur jene Belange aufgegriffen werden, auf die im Kernstück des Berichts näher eingegangen wird.

3.1.9. Nicht behobene Mängel der letzten Revision

Sofern alle in vorhergehenden Revisionsberichten erwähnten Schwachstellen zwischenzeitlich behoben worden sind, ist an dieser Stelle der Vermerk «keine» anzubringen. Die Revisionsüberschrift, die Berichtsnummer sowie das Berichtsdatum vorhergehender Revisionen sind ebenfalls zu vermerken.

Es ist grundsätzlich auf alle in vorhergehenden Revisionsberichten formulierten Anträge, die bis dato noch nicht umgesetzt wurden, hinzuweisen. Die Revisionsüberschrift, die Berichtsnummer sowie das Berichtsdatum vorhergehender Revisionen sind ebenfalls zu vermerken.

Falls zahlreiche zuvor in einem Management Letter rapportierte Schwachstellen noch nicht bereinigt worden sind, ist dies auch zu vermerken, falls der Revisionsverantwortliche der Ansicht ist, das Management räume der termingerechten Problembehebung zu wenig Bedeutung ein.

3.1.10. Risikobeherrschung

In jedem Revisionsbericht ist für die für das Risikomanagement der IT massgebenden 6 Standardrisikokategorien ein Risiko-Rating festzulegen. Sollte eine Risikokategorie nicht zutreffen, ist in der Spalte «Wirksamkeit des Risikomanagements» ein entsprechender Vermerk zu machen («nicht zutreffend»), oder kann ganz weggelassen werden.

Für jene Risikokategorien, deren Rating «mit Vorbehalt» oder «ungenügend» lautet, ist im Abschnitt «Wesentliche Feststellungen» des Berichts die Feststellungsnummer anzugeben.

<i>IT-Risikokategorie</i>	<i>Wirksamkeit des Risikomanagements</i>	<i>Gesamt-Bewertung</i>
Strategic		
Development		
IT Delivery		
Financial		

IT Organisation



Legal &
Compliance



Rating-Legende:

Grün = gut und zufriedenstellend; Gelb = mit Vorbehalt; Rot = ungenügend

3.1.11. Wesentliche Feststellungen

In den Abschnitt «Wesentliche Feststellungen» des Revisionsberichts gehören ausschliesslich wesentliche Feststellungen gemäss Management Letter (d. h. Feststellungen, die dem Senior Management zur Kenntnis zu bringen sind). Solche Feststellungen können finanzielle Verluste und/oder eine schwerwiegende Missachtung der Vorschriften beinhalten. Insofern handelt es sich hierbei in der Regel um Prüfungsziele, die entweder als «mit Vorbehalt» oder als «ungenügend» eingestuft wurden.

Die Überschrift für diesen Abschnitt des Berichts entspricht der Berichtskategorie, während die Unterkapitel den übergeordneten Prüfungszielen entsprechen.

Es ist darauf zu achten, dass die im Rahmen des Berichts erwähnten Feststellungen und Anträge mit den Angaben im Abschnitt «Prüfungsumfang» übereinstimmen.

Für den Fall, dass eine Revision wesentliche Schwachstellen zu Tage fördert, ist der Revisionsbericht um folgende Angaben zu ergänzen:

- möglichst knappe Zusammenfassung der Feststellungen
- kurze Ausführung zu den Risiken
- konkrete Anträge zur Behebung der gefundenen Schwachstellen
- Stellungnahme des Managements.

Am Ende des Abschnitts «Wesentliche Feststellungen» ist mit der folgenden Standardformel auf den Management Letter zu verweisen: «Für detaillierte Kommentare und Anträge wird auf den Management Letter (yy-nnnb) zuhanden des Managements verwiesen».

3.1.12. Stellungnahme: Direktion

Seitens des für den geprüften Bereich verantwortlichen Managements ist eine Stellungnahme einzuholen. Das verantwortliche Management genehmigt/kommentiert die im Revisionsbericht enthaltenen Angaben. Die für den Kommentar verantwortlichen Manager sind namentlich im Rahmen der Stellungnahme zu nennen. Des Weiteren sind deren Funktion sowie das Datum des Eingangs der Stellungnahme aufzuführen.

3.1.13. Stellungnahme: Geschäftsleitung

Bevor der Bericht durch die IT ASG herausgegeben wird, kann eine Stellungnahme seitens des Managements des Unternehmensbereichs eingeholt werden.

Das für den Unternehmensbereich verantwortliche Management genehmigt/kommentiert die im Rahmen des Revisionsberichts gemachten Angaben und verweist gegebenenfalls auf die Stellungnahme des verantwortlichen Managements. Die für den Kommentar verantwortlichen Manager des Unternehmensbereichs sind namentlich im Rahmen der Stellungnahme zu nennen. Des Weiteren sind deren Funktion sowie das Datum des Eingangs der Stellungnahme aufzuführen.

3.1.14. Stellungnahme: Konzernleitung

Stellungnahme/Schlusswort des CEO sowie weiterer Mitglieder der Konzernleitung.

3.1.15. Stellungnahme: Präsidium

Stellungnahme/Schlusswort des Verwaltungsratspräsidenten und des stellvertretenden Verwaltungsratspräsidenten.

3.2. Management Letters

3.2.1. Zweck

Durch Management Letters werden sämtliche Prüfungsfeststellungen einer Revision dem verantwortlichen Management zur Kenntnis gebracht, einschliesslich jener Feststellungen, die im Revisionsbericht zusammengefasst werden. Bezüglich Qualität und Quantität der Feststellungen und Anträge sind die für den Report gemachten Bemerkungen auch für den Management Letter, mit dem einzigen Unterschied, dass der Management Letter einen höheren Detaillierungsgrad mit mehr „Fleisch am Knochen“ aufweisen muss, in vollem Umfang verbindlich.

3.2.2. Form und Inhalt

Der an den für den geprüften Bereich verantwortlichen Manager gerichtete Management Letter beinhaltet, sofern vom Kunden nicht anders gewünscht, folgendes:

- Übermittlungsnotiz
- Audit Scorecard (Zusammenfassung der Revisiionsergebnisse nach übergeordneten Prüfungszielen)
- Ausführungen zur Revision, Revisionsanträge und Stellungnahme seitens des Managements
- Prüfungsumfang (optional) – mit über den Prüfungsumfang im Rahmen des Revisionsberichts hinausgehenden Angaben.

Für die Darstellung von Management Letter ist ein verbindliches Layout vorgegeben.

3.3. Memoranden

Ob nebensächliche, während einer Revision auftauchende Fragen dem für den betreffenden Unternehmensbereich zuständigen Management mittels eines Memorandums mitzuteilen sind, liegt im Ermessen des Revisionsverantwortlichen.

Auch Memoranden, durch die dem Management während einer Revision wichtige Belange sofort zur Kenntnis gebracht werden sollen, sind zuerst dem Leiter der IT ASG vorzulegen.



Memoranden, die der Kommunikation von Ausführungen der IT ASG im Anschluss an eine Prüfung von Projektdokumentationen/Konzeptabhandlungen (entweder im Rahmen einer Vorimplementierungsrevision oder der Entwicklung neuer Produkte) dienen, sind ebenfalls dem Leiter der IT ASG vorzulegen.