VAN ACKEN
UND PARTNER

Vortrag

# DV-SYSTEMPRÜFUNG
# VERSUS
# RISIKOORIENTIERTE PRÜFUNG

Jahresfachkonferenz DV-Revision
Risikomanagement und Effizienzbewusstsein
Hamburg

IT-SYSTEMPRÜFUNG · DATENANALYSE · IT-SICHERHEITSMANAGEMENT
VAN ACKEN + Partner G.m.b.H. & Co. · Offakamp 9a· 22529 Hamburg
Telefon (040) 55 76 28 55 · Telefax (040) 55 76 28 58 · E-Mail office@vanacken.de · Homepage: http://www.vanacken.de
Geschäftsführer: Dipl.-Kfm. Jan van Acken · Amtsgericht Hamburg HR A 89025
Komplementär: VAN ACKEN + Partner Beteiligungsgesellschaft m.b.H. · Amtsgericht Hamburg HR B 59521

**Inhalt**

Für Ihre Notizen

## A. Einleitung

Die zunehmende Komplexität der DV-Landschaft mit steigender Heterogenität und Offenheit der DV-Strukturen führt zu immer höheren Anforderungen an die DV-Revisoren.

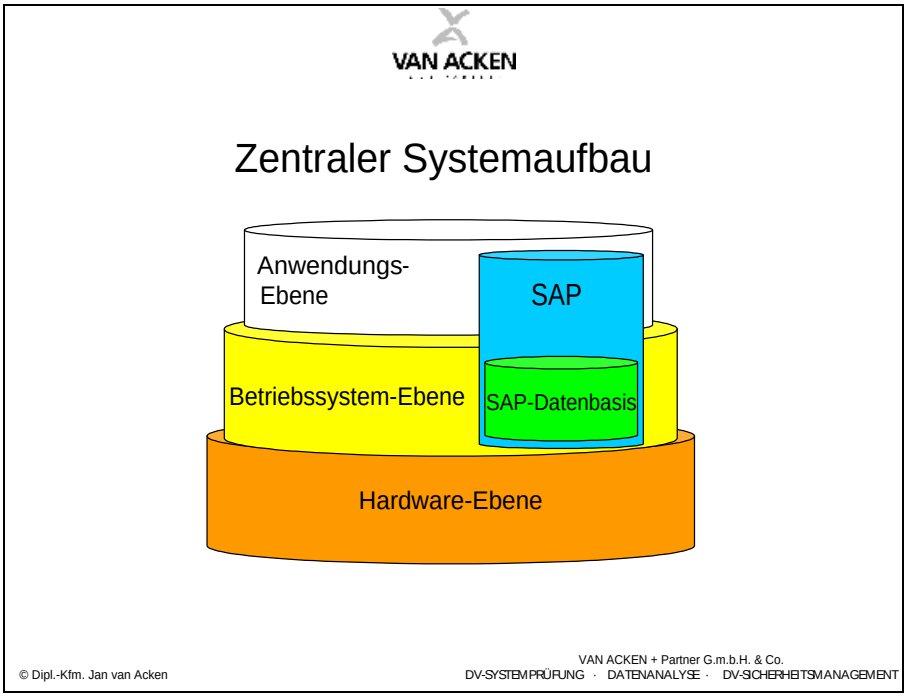



**Abbildung 1: Zentraler Systemaufbau**

Neuere DV-Systeme:

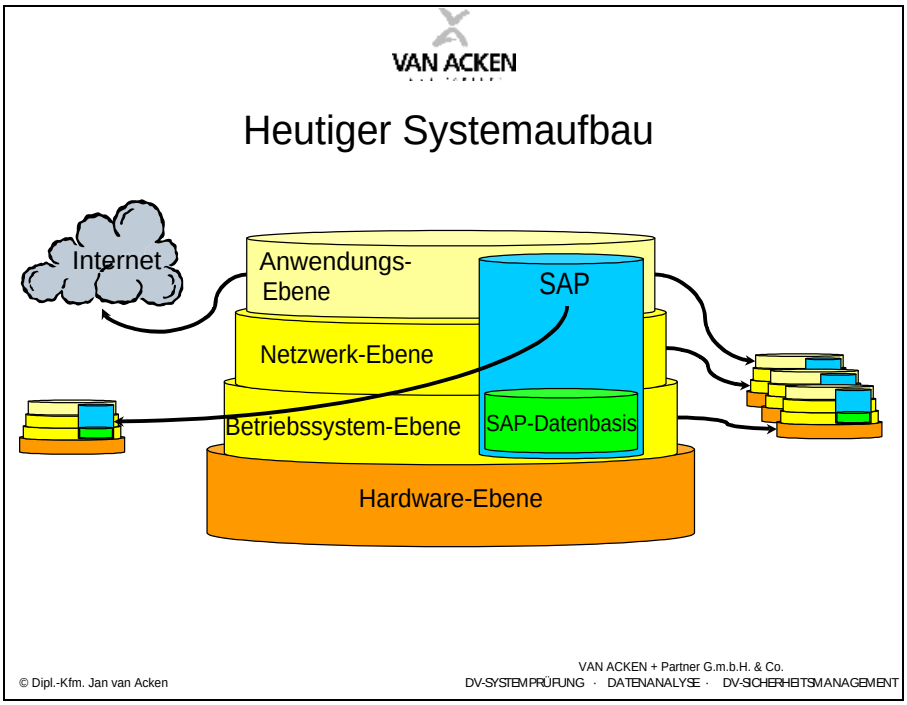



**Abbildung 2: Heutiger Systemaufbau**

Diese Anforderungen steigen darüber hinaus durch ein exponentiell ansteigendes Technologieniveau innerhalb der Unternehmen und, parallel dazu, zunehmender Abhängigkeit der Gesamtorganisation vom DV-Bereich. Hieraus folgt eine Risikoerhöhung für das gesamte Unternehmen.

Diese Ausgangssituation wird durch zeitlich engere Prüfungspläne sowie zunehmende Kosten/Nutzen-Betrachtungen der Revision an sich verschärft. Ein weiteres Problem ergibt sich durch die steigende Anzahl gesetzlicher Normen, wie beispielsweise das KonTraG[1], deren Umsetzung innerhalb der Unternehmen, wie in diesem Falle, insbesondere durch die Revision zu erfolgen hat. Hierdurch kommt es zu einer sich immer weiter öffnenden Schere zwischen den Anforderungen an die DV-Revision auf der einen Seite und dem zunehmenden Kostendruck sowie den eingeschränkten Ressourcen der Revision innerhalb der Unterneh-

1 KonTraG steht für Gesetz zur Kontrolle und Transparenz im Unternehmen. Den Gesetzestext finden Sie unter http://www.datenschutz-und-datensicherheit.de/dudserver/datensicherheit.htm.

men auf der anderen Seite.

In den Kerngeschäftsbereichen der Unternehmen ist Personalabbau zur Kosteneinsparung eine wesentliche Maßnahme, die auch vor den Stabstellen der Unternehmen nicht Halt macht.

*Wie sollen bei dieser Ausgangslage die Revisionsabteilungen den noch steigenden Qualitätsansprüchen gerecht werden?*

Ein in dieser Entwicklung fortgeschrittener Wirtschaftsraum ist der der Vereinigten Staaten. Er wird im Bereich der Revision der Banken dem der Bundesrepublik Deutschland wie folgt gegenübergestellt:

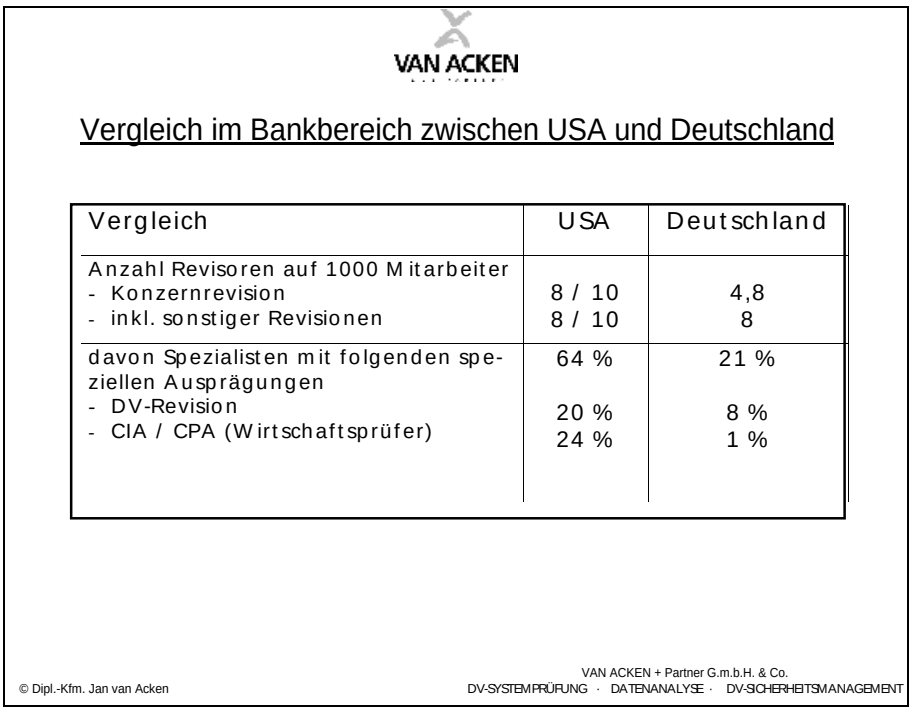



**Abbildung 3: Vergleich im Bankbereich zwischen USA und Deutschland[2]**

Folgende Trendsituationen sind hieraus hinsichtlich der USA direkt ablesbar:

1. Die Konzentration der Revisionsaufgaben im Konzern;
2. eine deutlich höhere Spezialisierung der Revisoren und

2 Vgl. Christian Grebien, Interne Konzernrevision im Bankbereich, in: Interne Revision, Jg. 34, Heft 2a.1999, Seite 20-28.

3. ein höherer Ausbildungsstand der Revisoren.

Zu beachten ist, daß dieser Entwicklungstrend in den USA lediglich einen Hinweis auf mögliche Entwicklungen in Deutschland zuläßt.

Unter Berücksichtigung der Standortgegebenheiten innerhalb der Bundesrepublik Deutschland ist der Aufgabenbereich und damit das oben skizzierte Spannungsfeld der Revision durch folgende beeinflussende Faktoren gekennzeichnet:

- Gesetzliche Grundlagen,
  - Stellungnahmen und Verlautbarungen,
- Unternehmensinterne Veränderungen,
  - verfügbare Ressourcen,
  - Aufbau- und Ablauforganisation,
- potenziell zu nutzende Methoden und Verfahren im Bereich der Revision.

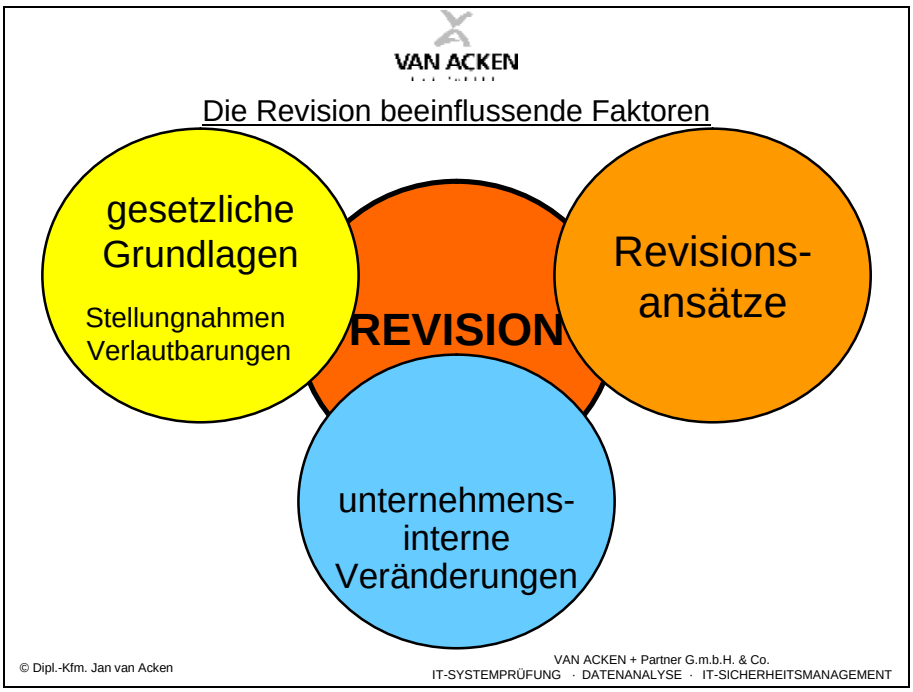



**Abbildung 4: Die Revision beeinflussende Faktoren**

Um zu einer detaillierteren Betrachtungsperspektive dieser Ausgangssituation zu gelangen, ist es notwendig, die sich ergebenden beeinflussenden Bereiche genauer zu betrachten.

Wenn ich nun mit den gesetzlichen Grundlagen beginne, knüpfe

Für Ihre Notizen

ich damit an die Ausführungen meines Vorredners, Herrn Heese, an. Die gesetzlichen Grundlagen, Stellungnahmen und Verlautbarungen zum Thema der DV-Revision stellen einerseits die rechtlich einzuhaltenden Rahmenbedingungen dar und zeigen andererseits für den DV-Revisor einen extern vorgegebenen Maßstab auf, an dem er seine Prüfungshandlungen orientieren kann.

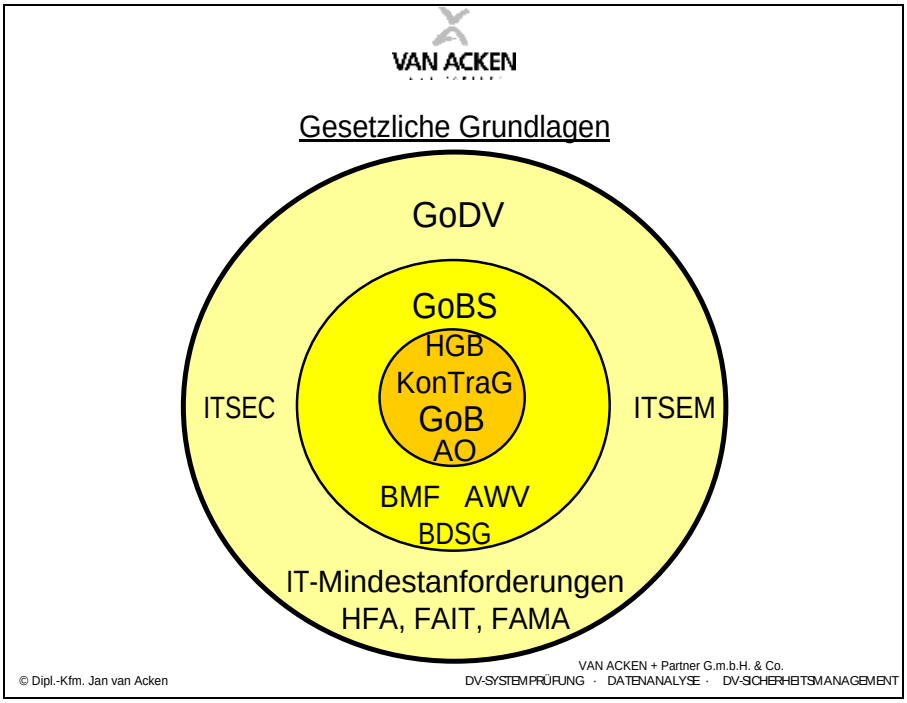



**Abbildung 5: Gesetzliche Grundlagen**

Im engeren Sinne handelt es sich hierbei um die gesetzlichen Normen, die zusammengefasst den Begriff der GoB ergeben. Speziell auf den Bereich der DV-Revision bezogen, kommen die Stellungnahmen und Verlautbarungen hinzu, die unter dem Begriff der GoBS zu subsumieren sind. Gehen wir nun im Folgenden von dem von Herrn Schuppenhauer[3] geprägten Begriff der GoDV aus. Er erweitert die zuvor genannten GoBS noch um hinzukommende Stellungnahmen und Verlautbarungen. Hier sind beispielsweise die des Instituts der Wirtschaftsprüfer in Deutschland e.V.(zukünftig kurz IDW) oder die nationalen und

3 Vgl. Rainer Schuppenhauer, Grundsätze für eine ordnungsmäßige Datenverarbeitung (GoDV), 4. Aufl., Düsseldorf 1992.

internationalen Sicherheitsanforderungen, die in Deutschland durch das Bundesamt für Sicherheit in der Informationstechnik gesetzt werden, zu nennen.

Abhängig davon, welche dieser gesetzlichen Normen, Stellungnahmen und Verlautbarungen auf Grund

- des Unternehmenseigentümers,
- der Unternehmensrechtsform und
- des Unternehmensstandortes

greifen, sind unterschiedliche gesetzliche Normen vom Unternehmen zu erfüllen, wie beispielsweise ein bestimmter Standard nach ITSEM[4] oder ITSEC[5].

Für die Revision stellt sich dieser Bereich als nicht zu beeinflussende Vorgabe dar, deren Erfüllung Prüfungsgegenstand ist. Es besteht hier keine Möglichkeit, innerhalb des Unternehmens Einfluss nehmen zu können.

Auch die unternehmensinternen Veränderungen und Vorgaben stellen aus Sicht der Revision keine Möglichkeit für effizienzsteigernde Maßnahmen dar, sondern sind als Vorgaben der Revisionsarbeit zu sehen. Darüber hinaus gilt für diesen wie für den zuvor skizzierten Bereich der gesetzlichen Grundlagen, dass die sich in diesen Bereichen ergebenden Änderungen direkt von der Revision wahrgenommen und in eigene Prüfungshandlungen umgesetzt werden müssen. Für den Bereich der unternehmensinternen Veränderungen ergibt sich folgendes Bild:

4 ITSEM steht für Information Technology Security Evaluation Manual. Sie finden die aktuelle Version unter http://www.bsi.de/zertifiz/itkrit/itsem-dt.pdf

5 ITSEC steht für Information Technology Security Evaluation Criteria. Sie finden die aktuelle Version unter http://www.bsi.de/zertifiz/itkrit/itsec-dt.pdf

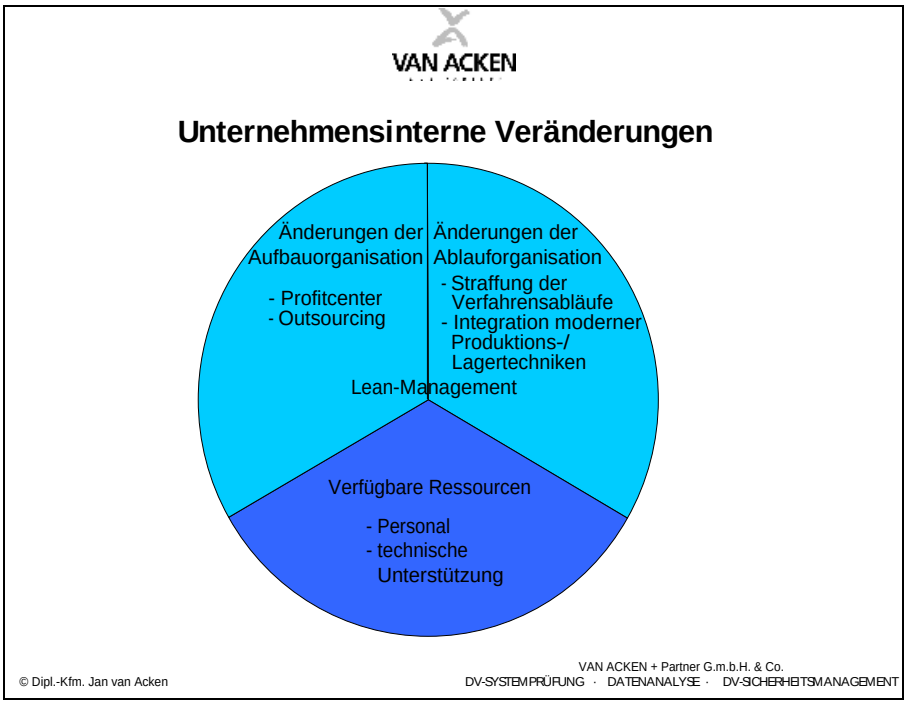



**Abbildung 6: Unternehmensinterne Veränderungen**

Die in Unternehmen möglichen Veränderungen sind zum einen durch die hier hellblau dargestellten indirekten Einflußfaktoren und zum anderen durch die dunkler hinterlegten direkten Einflußfaktoren bedingt.

Bei den direkten Einflußfaktoren handelt es sich um das zur Verfügung stehende Personal sowie die technische Unterstützung der Revisionstätigkeit innerhalb der Organisation. Sie bilden damit die verfügbaren Ressourcen der gesamten Revisionstätigkeit innerhalb des Unternehmens oder der Unternehmensgruppe.

Zum anderen beeinflussen Änderungen der Aufbauorganisation, beispielsweise durch das Outsourcing von Teilbereichen, z.B. der Rechenzentrumsleistung des Unternehmens, oder die Umstrukturierung des gesamten Unternehmens in einzelne, in einer Holding zusammengeführten Profitcenter die Tätigkeiten der Revision indirekt. Das Gleiche trifft auch auf Änderungen innerhalb der Ablauforganisation zu, sei es durch Straffung von Verfahrensabläufen, durch Integration moderner Produktions- und Lagertechniken oder durch die in neuerer Zeit als Schlagworte anzusprechenden Tendenzen der Dezentralisierung, der Kunden-

orientierung, des Prozessengeneering, der Internationalisierung und damit nicht zuletzt der Anpassung der Organisation an die Globalisierung der Märkte.

Wie oben bereits erwähnt, stellen diese unternehmensinternen Rahmenbedingungen Vorgaben für die Revisionstätigkeit dar. Sie repräsentieren zum einen im Bereich der direkten Einflußmöglichkeiten das untere Feld, mit dem innerhalb des Unternehmens überhaupt Revision betrieben werden kann. Zum anderen handelt es sich bei den indirekten Faktoren um die Bereiche, die die Tätigkeit der Revision durch den Zwang der Anpassung der revisionsinternen Methoden und Verfahren beeinflussen.

Unter den vorher zitierten Rahmenbedingungen besteht nun die eigentliche Flexibilität der Revision in der Wahl der richtigen Prüfungsansätze. Darum sollen im Folgenden die Methoden und Verfahren der DV-Systemprüfung, das Vorgehen bei der Ex-ante- und Ex-post-Prüfung sowie die Festlegung des optimalen Prüfungszeitpunktes für unterschiedliche Prüfungsbereiche erläutert werden.

Für Ihre Notizen

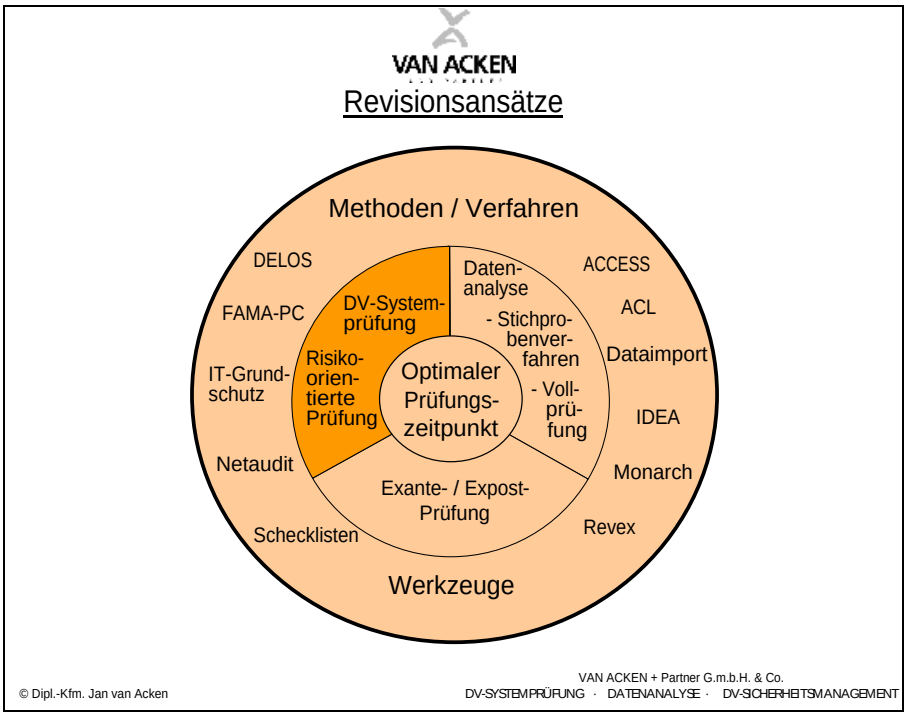



**Abbildung 7: Revisionsansätze** [6]

Aus dem Gesamtspektrum der Revisionsansätze soll nun die DV-Systemprüfung sowie der risikoorientierte Ansatz dargestellt und zueinander in Beziehung gesetzt werden. Dieses ist, wie die folgenden Ausführungen zeigen werden, ausschließlich unter Berücksichtigung der gerade angesprochenen gesetzlichen Regelungen sowie der vorliegenden Organisationsform des Unternehmens sinnvoll möglich.

6 Weiterführende Literatur: Heinz Königsmaier, Der optimale Prüfzeitpunkt in der Internen Revision – eine Untersuchung des „audit timing-Problems“ aus theoretischer Sicht, in: Zeitschrift für Interne Revision 2a, 34. Jg., 1999.

## B. DV-Systemprüfung

Die DV-Systemprüfung ist eine Verfahrensprüfung. Sie prüft nicht die korrekte Verarbeitung eines einzelnen Geschäftsvorfalles, sondern die organisatorisch gesicherte Zuverlässigkeit eines Teil- oder des Gesamtsystems.

Um diesen Gedanken zu vertiefen, sind folgende Vorüberlegungen notwendig:

Geteilte Systeme wie alle computergestützten Verfahren sind dadurch gekennzeichnet, dass die Geschäftsvorfälle in eine maschinenlesbare Form gebracht und anschließend verarbeitet, gespeichert und zwecks Anzeige oder Ausdrucks wieder lesbar gemacht werden. Das Überführen von Geschäftsvorfällen in maschinenlesbare Form auf den zu betrachtenden Rechner kann entweder durch manuelle Eingabe eines Benutzers, automatisch per Datenfernübertragung oder aber teilautomatisiert durch Übernahme per Erfassungsbeleg oder Scanner erfolgen. Gleiches Systemumfeld vorausgesetzt, ist somit der Schluss zulässig, dass die in den Programmen niedergelegten Anweisungen und Kontrolltechniken regelmäßig die gleichen Ergebnisse bewirken.

Diese Deterministik legt den Schluss nahe, dass Datenverarbeitung richtig und vollständig erfolgt, wenn fehlerfreie Programme richtige und vollständige Eingabedaten im Rahmen störungsfrei arbeitender Hardware verarbeiten.

Als Maßstab für den ex- als auch internen Prüfer der zu prüfenden Systeme gelten beispielsweise die zuvor beschriebenen Stellungnahmen und Verlautbarungen sowie die GoBS. Die hier erhobenen Forderungen stützen sich auf die technische Lösung, die die Einhaltung der Forderungen garantieren soll, sowie auf die Dokumentation der Lösung. Dabei lassen alle Verlautbarungen die Möglichkeit von Mängeln in der technischen Lösung bei gleichzeitig erfolgenden umfassenden und widerspruchsfreien Arbeitsanweisungen zu. Grundsätzlich gilt hierbei, wenn eine ausreichende Dokumentation des Verfahrens vorliegt und aus-

reichende Kontrollen die Einhaltung der Arbeitsanweisungen gewährleisten und diese Kontrollen wiederum dokumentiert sind, entspricht das vorliegende System den Anforderungen. Dabei sollen die Kontrollen möglichst technisch durch laufende Dokumentationen in Form von LOG-Dateien durchgeführt werden, die wiederum weitestgehend alle im Anwendungsprogramm sowie auf Netzwerkebene vorhandenen Tätigkeiten aufzeichnen. Dabei sind die Kontrollen sowie deren Umfang, die Ergebnisse der Kontrollen sowie die Intervalle, in denen mindestens zu kontrollieren ist, Bestandteil der Dokumentation und zu archivieren.

## B.1. Vorbereitung der DV-Systemprüfung

Grundlegend lassen sich zwei Anwendungsprüfungen unterscheiden:

- Ex-post-Prüfung,
- Prüfung von DV-Vorhaben (Ex-ante-Prüfung).

Abhängig von der Art der Anwendungsprüfung ergeben sich unterschiedliche Vorgehensweisen bei der Prüfungsvorbereitung.

Die Vorbereitung sowie die Vorgehensweise bei der Prüfung von DV-Vorhaben lehnt sich direkt an die Entwicklung oder Auswahl des neu einzusetzenden DV-Vorhabens an und ist daher in direkter Zusammenarbeit mit den zukünftigen Nutzern zu planen und abzustimmen.

Während die Prüfung von DV-Vorhaben die geplante Umsetzung eines DV-Vorhabens aus Prüfersicht begleitet, bezieht sich die Ex-post-Prüfung ausschließlich auf bereits freigegebene DV-Systeme.

Für Ihre Notizen

## B.2. Ex-post-Prüfung

Die Vorbereitung der Ex-post-Prüfung beginnt grundsätzlich mit dem Schritt der Konkretisierung des Prüfungsauftrages. Hierbei wird erneut das Prüfungsziel definiert und davon abgeleitete Prüfungsschwerpunkte festgelegt .

Anhand des Prüfungszieles und der vereinbarten Schwerpunkte wird nun vom Prüfer die Vorgehensweise ausgearbeitet. Gehen wir beispielhaft vom Prüffeld der Anwendersoftware aus, wären hier in der Abfolge folgende beispielhafte Bereiche zu prüfen:

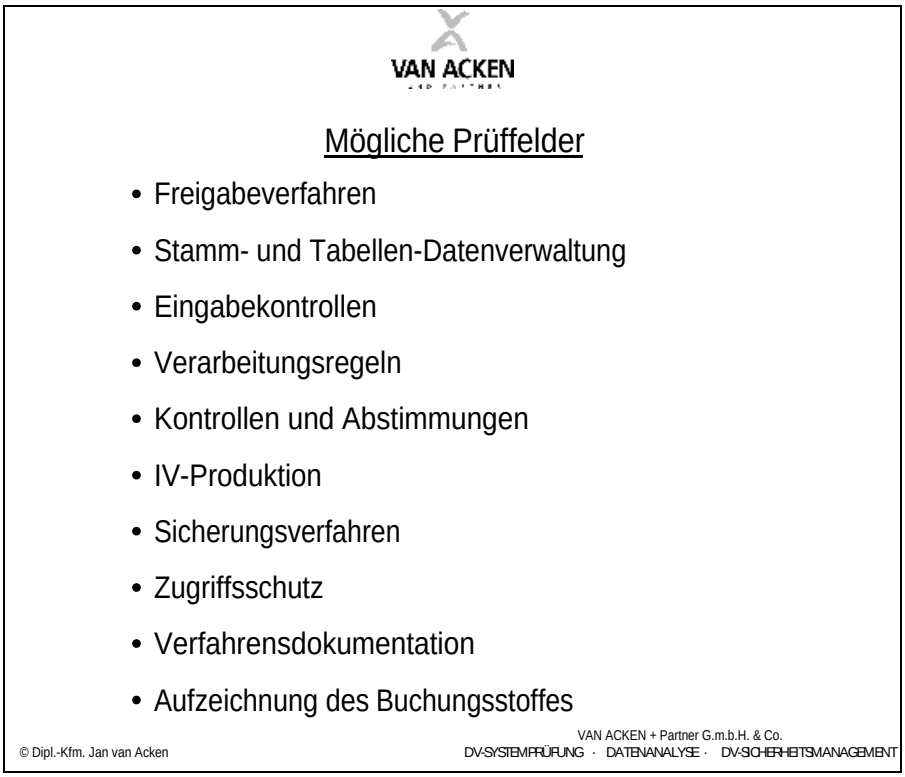



**Abbildung 8: Mögliche Prüffelder**

Wie oben bereits angesprochen, wäre ein mögliches Prüffeld der Zugriffsschutz bzw. die Zugriffsrechte von Mitarbeitern. Hierzu sind die Aufgaben der einzelnen Mitarbeiter zusammenzufassen und den Zugriffsrechten auf Betriebssystem-, Netzwerk- und Anwenderebene gegenüberzustellen.

Für Ihre Notizen

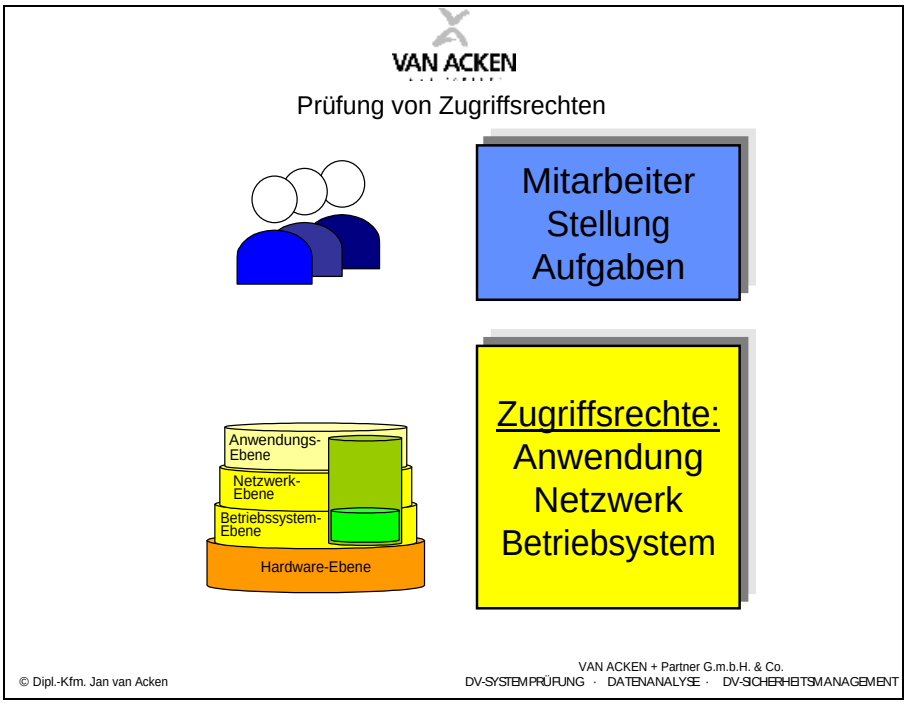



**Abbildung 9: Prüfung von Zugriffsrechten**

Bei diesem Abgleich kommt es insbesondere auf die Übereinstimmung der Aufgabenbereiche des Mitarbeiters mit seinen Rechten auf allen DV-technischen Ebenen an. Darüber hinaus ist das Vorhandensein von Mitarbeitern mit Zugriffsrechten ohne Arbeitsplatz im Unternehmen oder die doppelte Existenz von DV-technisch angelegten Mitarbeitern innerhalb des Unternehmens zu prüfen.

Als nächster Schritt ist die Bereitstellung von Prüfungshilfsmitteln zu garantieren. Hierunter fallen zum einen die vom Prüfer selbst zu organisierenden Hilfsmittel, also beispielsweise Gesetzestexte, GoBS oder das Wirtschaftsprüferhandbuch. Zum anderen sollte spätestens an dieser Stelle des Ablaufes Verbindung mit der zu prüfenden Organisation oder Abteilung aufgenommen werden. Ziel dieser Kontaktaufnahme ist die Abstimmung über die zur Prüfung von der Organisation zu erbringenden Leistungen. Hierzu kann beispielsweise zählen:

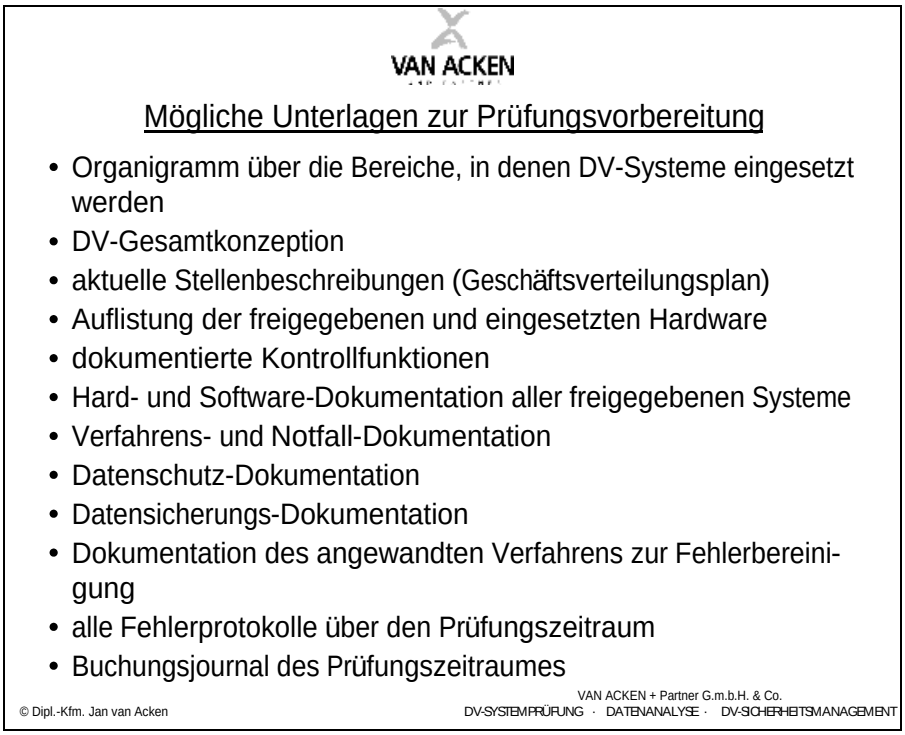



**Abbildung 10: Mögliche Unterlagen zur Prüfungsvorbereitung**

Die praktische Erfahrung hat gezeigt, dass diese Verbindungsaufnahme circa sechs Wochen vor der eigentlichen Prüfung stattfinden sollte. Ihr Ziel besteht neben der Übermittlung der für die Prüfung notwendigen Anforderungen insbesondere darin, in einem Gespräch die Anforderungen näher zu erläutern und damit auch die gegebenenfalls vorhandenen Vorbehalte hinsichtlich des zu prüfenden Bereichs abzubauen. Auch sollte man einen ersten Eindruck über die Organisation der dort eingesetzten Hard- und Softwareumgebung erlangen, damit der Prüfer den eigentlichen Prüfungseinsatz besser vorbereiten kann.

Nach Erhalt der ersten Informationen sollte vor Prüfungsbeginn ein vorzugebender Soll-Zustand vom Prüfer festgelegt werden. Im Bereich der Systemprüfung von Buchhaltungssystemen wäre hier der Maßstab der GoBS zu nennen. In Abhängigkeit vom Prüfungsauftrag und Prüfungsziel sind aber auch andere, vom Prüfer selbst zu erstellende Maßstäbe denkbar.

Nach diesen Vorarbeiten beginnt dann die eigentliche Prüfung,

die wiederum in zwei Bereiche zerfällt. Zum einen findet eine Verfahrensprüfung mit dem Ziel statt, den Ablauf von der Dateneingabe bis zur Datenausgabe aufzuzeigen. Zum anderen fallen hierunter alle Prüfungshandlungen, die parallel dazu notwendig sind, um den mit dem Datenfluss verbundenen organisatorischen Bereich transparent zu machen.

Hierzu kann der Prüfer eine Reihe von Hilfsmitteln nutzen, wie beispielsweise die Fragenkataloge innerhalb der Programme FAMA-PC, des IDW oder das auf ähnlichen Checklisten basierende Produkt Delos der DATEV.

Die hier angesprochenen, an Checklisten orientierten, Hilfmittel unterstützen den Prüfer lediglich dabei, eine höhere Transparenz über die zu prüfende Organisation zu erlangen. Darüber hinaus sind meistens insbesondere im Bereich der Schnittstellenprüfungen Datenübernahmen und -analysen unumgänglich. Hierzu stehen dem Prüfer neben den üblichen Datenbanken Werkzeuge wie DEA oder ACL zur Verfügung.

Nur eine Ergänzung der klassischen DV-Systemprüfung durch die Datenanalyse für die hierbei erkannten Schnittstellen und Problembereiche ermöglicht ein abschließendes Bild über den zu prüfenden Bereich.

Hieraus ergibt sich nochmals zusammengefasst folgende Vorgehensweise:


**Abbildung 11: Vorgehensweise bei der DV-Systemprüfung**

Alle bei der Prüfung zusammengetragenen Erkenntnisse sollten abschließend einer kritischen Würdigung, also der Gegenüberstellung des SOLL- mit dem IST-Zustand unterzogen werden. Sie mündet letztendlich in die Berichterstattung, bei der die einzeln aufgeführten Feststellungen bewertet werden sollten. Hieraus folgen schließlich Vorschläge für das weitere Vorgehen.

## B.3. Projektbegleitende Prüfung (Ex-ante-Prüfung)

Der Bereich der projektbegleitenden Prüfung soll hier nur als Ergänzung, da er Teil der DV-Systemprüfung ist, erwähnt werden. Er hat aber im Vergleich zum risikoorientierten Ansatz keinerlei Bedeutung.

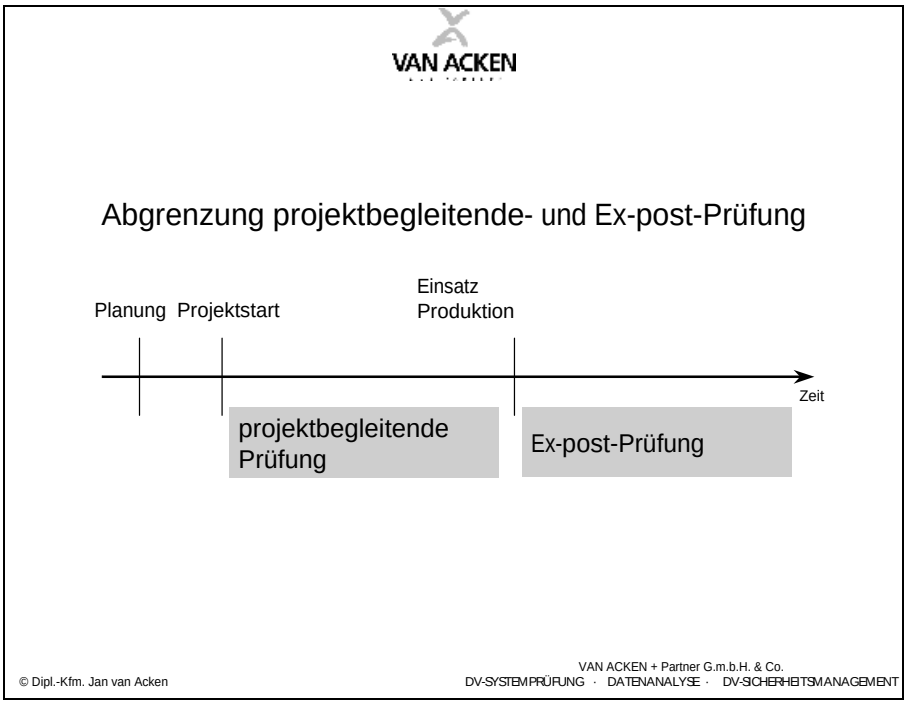



**Abbildung 12: Abgrenzung projektbegleitende und Ex-post-Prüfung**

Bei der projektbegleitenden Prüfung stehen nicht bereits freigegebene Verfahren im Vordergrund, sondern diese Prüfung setzt im Zeitablauf bereits bei der Erstellung der Programmanforderungen (Pflichtenheft) ein. Das heißt, sie erstreckt sich über den gesamten Zeitraum des Programmfreigabeverfahrens. Diese gliedert sich in die Bereiche

- Programmanforderung,
- Versionsfortschreibung,
- Anlass und Inhalt der Änderung,
- Testverfahren,
- Freigabe durch Fachabteilung,
- Freigabe durch DV-Revision und Qualitätssicherung,
- Übergabe an Produktion,
- Zeitpunkt der Inbetriebnahme.

Im Gegensatz zur Ex-post-Prüfung, die in das Rechtssystem stark eingebunden ist, steht der Prüfer hier einem Bereich gegenüber, der neben großen Freiräumen auch ein großes Risiko beinhaltet. Er nimmt dabei neben der Perspektive des Prüfers

auch die des für die Revision verantwortlichen Beraters ein.

Lassen Sie mich hierzu anmerken, dass in Hinblick auf die Effizienzsteigerung der gesamten Revisionstätigkeit eine Verlagerung von der Ex-post- -unabhängig welches Verfahren Sie hierbei zu Grunde legen - hin zur Ex-ante-Prüfung unumgänglich scheint.

**Zusammenfassung**

Wie dargestellt ist die DV-Systemprüfung eine Verfahrensprüfung, deren Ziel die Analyse von Abläufen und Informationsströmen innnerhalb einer Teilorganisation oder Organisation ist.

Technisch wird der Revisor durch Checklisten oder DV-technische Werkzeuge, die weitestgehend auf automatisierten und in erweiterten Versionen selbst anpassbaren Checklisten-Systemen beruhen, unterstützt.

Darüber hinaus erfährt er eine Unterstützung durch Werkzeuge der Datenanalyse, wie beispielsweise IDEA, ACL oder jede Form von Datenbanken.

Unabhängig mit welchen der oben genannten Unterstützungen der Revisor arbeitet, liegt die Kreativität seiner Arbeit in der Anpassung und Erweiterung der vorliegenden Checklisten-Systeme und damit in der Abstimmung seines Prüfungsvorgehens auf das vorliegende Prüfungsobjekt.

Aus unserer Sicht ist eine DV-Systemprüfung nur mit Unterstützung der Datenanalyse erfolgreich, da nur so Schnittstellen näher analysiert und Manipulationen von Daten aufgedeckt werden können.

## C. Die risikoorientierte Prüfung

Im Folgenden soll das Risiko[7] - hier verstanden als die Möglichkeit, dass Aktivitäten, die körperlichen oder materiellen Schaden oder Verlust zur Folge haben oder mit anderen wirtschaftlichen Nachteilen verbunden sind betrachtet werden. Dabei sind beispielsweise folgende mögliche Risiken denkbar:

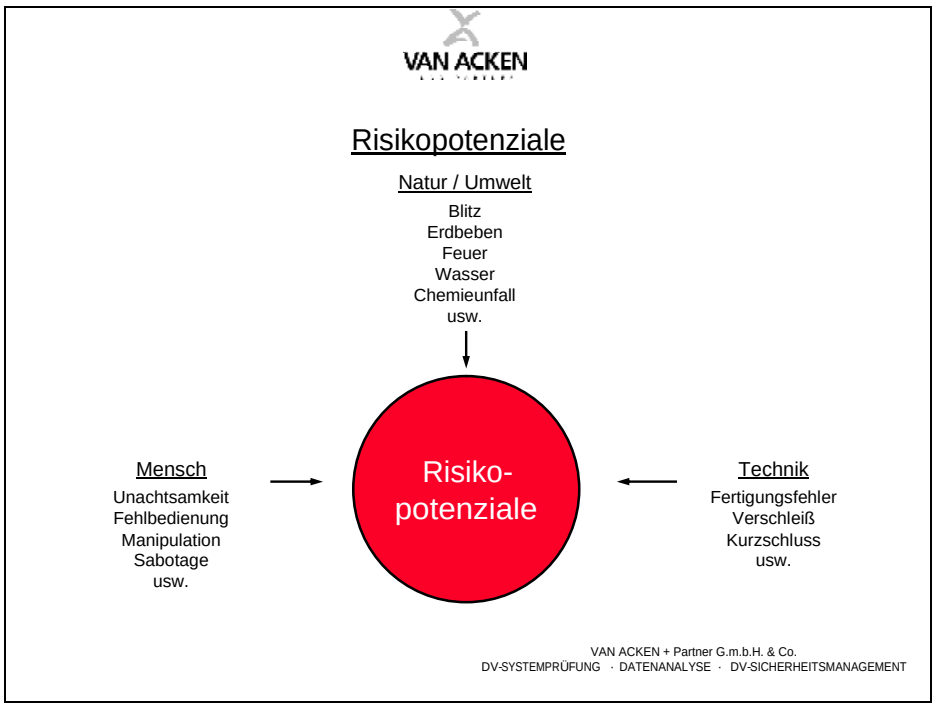



**Abbildung 13: Risikopotentiale**[8]

In diesem Sinne gilt ein Risiko dann als existent, wenn Bedrohungen vorliegen, denen keine adäquaten Maßnahmen entgegengesetzt werden, also wenn eine Schwachstelle besteht.

Die risikoorientierte Prüfung geht von der unternehmensindividuellen Betrachtungsweise aus. Als Voraussetzung für dieses

---

7 Vgl. Eva Stibi, Prüfungsrisikomodell und Risikoorientierte Abschlußprüfung, IDW-Verlag GmbH, Düsseldorf 1995 und
Kirsten Sell, Die Aufdeckung von Bilanzdelikten bei der Abschlußprüfung, Schriften des Instituts für Revisionswesen der Westfälischen Wilhelms-Universität Münster, hrsg. Jörg Baetge, Düsseldorf, 1999.

8 Vgl. Jürgen de Haas und Sixta Zerlauth, DV-Revision, Ordnungsmäßigkeit, Sicherheit und Wirtschaftlichkeit von DV-Systemen, Hrsg. Stefan Fedtke, Anzing, 1999, Seite 43 ff.

Verfahren ist die Ermittlung der bestehenden Risiken auch für einzelne Teilbereiche, z.B. ausschließlich für ein Anwendungsmodul innerhalb der gesamten Datenverarbeitung zu nennen.

### C.1. Abhängigkeitsanalyse

Vor der eigentlichen Risikoanalyse sollte eine Abhängigkeitsanalyse durchgeführt werden. Hierbei werden die unternehmensspezifischen Anforderungen an die Sicherheit der Datenverarbeitung ermittelt.

Im Rahmen der Abhängigkeitsanalyse werden folgende Ebenen betrachtet:

- Die Ebene der Ablauforganisation
  Hier werden insbesondere die Schnittstellen zwischen einzelnen Organisations- und Funktionseinheiten und deren DV-Unterstützung untersucht.
- Die Ebene der DV-Anwendungen
  Insbesondere hier gilt es, die Schnittstellen untereinander sowie deren Soft- und Hardware-technische Realisierung zu analysieren.
- Die Ebene der DV-Systeme und deren Vernetzung
- Die Ebene der Infrastruktur
- Die Ebene der Versorgungseinrichtungen, der technischen und baulichen Gegebenheiten

Das Modell der Abhängigkeitsanalyse zielt auf eine verlässliche und vor allem vollständige Untersuchung der Verfügbarkeit, der Integrität sowie der Verlässlichkeit einzelner Anwendungen und deren Daten. Auf Basis der Abhängigkeitsanalyse werden spezifische Anforderungen an die Sicherheitskriterien formuliert.

### C.2. Vorgehen bei der Risikoanalyse

Die Risikoanalyse gliedert sich in folgende Abschnitte:

- Systemabgrenzung,
- Bedrohungsanalyse,

- Schwachstellenanalyse.

Mit diesen Punkten sollen die Risiken für das Unternehmen aufgedeckt werden. Dabei kann eine der Bedrohungsanalyse folgende Risikobewertung dazu beitragen, die Höhe der möglichen Schäden und deren Häufigkeit individuell für die jeweilige Organisation abzuschätzen und somit für eine Priorisierung der Risiken und eine Bestimmung der Restrisiken zu sorgen. Abschließend folgt nach der eigentlichen Risikoanalyse die Erstellung eines Maßnahmenkataloges und dessen Umsetzung.

**Systemabgrenzung**

Innerhalb der Systemabgrenzung ist zu prüfen, ob das zuvor festgelegte Prüfungsobjekt aus der Risikoperspektive von den in der Verarbeitung vor- und nachgelagerten Bereichen abgegrenzt werden kann. Ggf. muss das Gesamtsystem hierzu segmentiert werden. Ziel der Segmentierung ist die Zergliederung in Subsysteme, wobei jedes einzelne dieser Systeme eine stark reduzierte Komplexität aufweist, so dass dieser Bereich übersichtlich erfassbar und darstellbar ist. Hierbei sind insbesondere auch die Abhängigkeiten der einzelnen Subsysteme zu berücksichtigen.

Nach dieser Zergliederung erhält der Revisor nicht nur einzelne, überschaubare Segmente, sondern auch eine Übersicht über alle Schnittstellen zwischen den zu betrachtenden Segmenten.

**Bedrohungsanalyse**

Die Bedrohungsanalyse soll die Einschätzung von Bedrohungen - zum Beispiel die Zerstörung von DV-Objekten wie Programmdaten, Hardware und andere -aufzeigen und diesen Bedrohungswerte zumessen. Dabei kommt es nicht nur auf die einzelne Bedrohung, sondern auch auf die daraus resultierenden Abhängigkeiten an. Dabei ist das Ziel der Bedrohungsanalyse, eine auftretende Bedrohung in einer der nachfolgenden Gruppen

als eine Menge innerbetrieblicher Schwachpunkte zusammenzufassen:

1. Preisgabe der Daten
2. Stillstand der DV-Infrastruktur
3. Manipulation und Datenverluste
4. Zeitdiebstahl und
5. Diebstahl von DV-Ressourcen

Alle diese Gruppen sind in drei Grundbedrohungen zusammengefasst:

- Verlust der Verfügbarkeit
- Verlust der Funktionssicherheit
- Verlust der Datensicherheit.

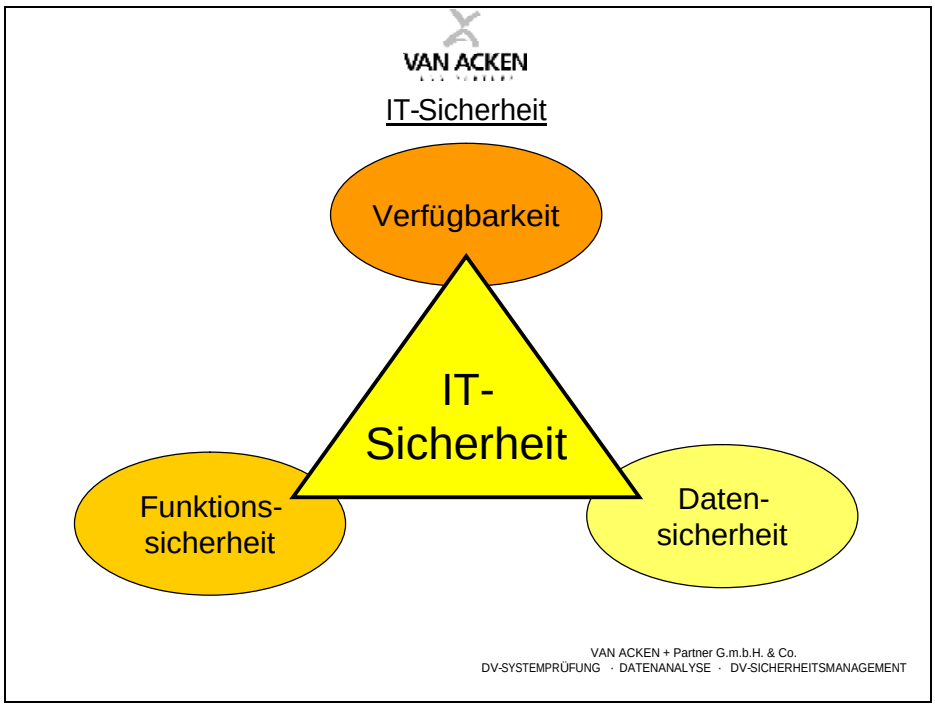



**Abbildung 14: IT-Sicherheit**[9]

Sie bilden zusammengefasst den Begriff der IT-Sicherheit.

Nachdem oben durch die fünf dargestellten Punkte verdeutlicht wurde, was bedroht sein kann, ist nun der Frage nachzugehen,

9 Vgl. Jürgen de Haas und Sixta Zerlauth, DV-Revision, Ordnungsmäßigkeit, Sicherheit und Wirtschaftlichkeit von DV-Systemen, Hrsg. Stefan Fedtke, Anzing, 1999, Seite 45 ff.

Für Ihre Notizen

worin die Bedrohung im Einzelnen besteht.

Es kann zwischen willkürlicher und vorsätzlicher Bedrohung unterschieden werden, wobei hier unter Willkür alle die Schäden zusammengefasst werden, die durch menschliches Versagen wie Bedienungs- und Tippfehler - beispielsweise eingearbeitete Artikelnummer als Artikelpreis - oder durch natürliche Einflüsse wie Naturkatastrophen und Verschleiß verursacht werden.

Im Gegensatz zur willkürlichen Bedrohung ist die vorsätzliche Bedrohung schwer zu beurteilen, da die Gefahr vom Denken und Handeln anderer Menschen ausgeht. Um in diesem Punkt dennoch zu einem Ergebnis zu gelangen, muss die Frage nach möglichen Tätern, deren Motiven sowie damit verbundenen Schäden beantwortet werden.

Das Ziel dieser Vorgehensweise besteht darin, den Grad der Bereitschaft zu ermitteln, bis zu dem der Schaden vom Unternehmen zu tragen und zu akzeptieren ist. Hierdurch ergibt sich die wirtschaftliche Betrachtungsweise der Bedrohungsanalyse.

Für Ihre Notizen

**Bestimmung des Restrisikos**

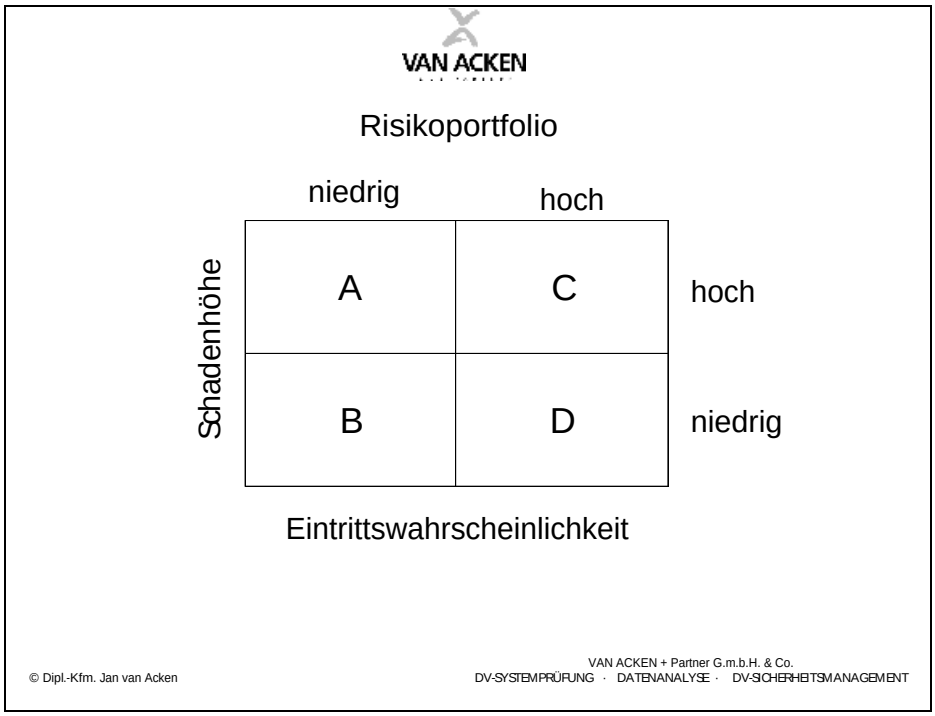



**Abbildung 15: Risikoportfolio**

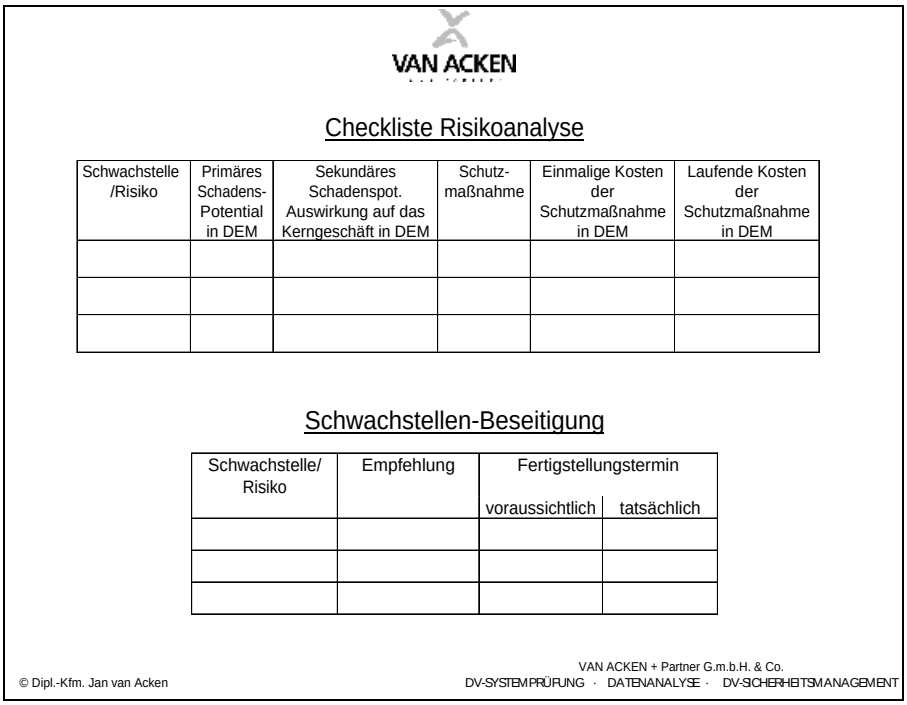
Da es grundsätzlich nicht möglich oder wirtschaftlich nicht vertretbar ist, allen Bedrohungen durch entsprechende Maßnahmen zu begegnen, bleiben zwangsweise Restrisiken, die bewusst toleriert werden. Weitestgehend läßt sich diesen Restrisiken durch deren Eintrittswahrscheinlichkeit sowie durch die anfallenden Kosten entgegenwirken. Oder anders ausgedrückt: Sind die sich ergebenden Risiken auf die Begriffe Schadenhöhe und Schadeneintrittswahrscheinlichkeit zu beziehen , kann sich ein Portfolio ergeben.

Bei den Restrisiken sind die bereits installierten Sicherheitsmaßnahmen oder die durch geringen zusätzlichen Aufwand zu installierenden Maßnahmen einzubeziehen.

**Schwachstellenanalyse**

Unter Berücksichtigung der eben erarbeiteten Ergebnisse ist nun eine Analyse der verbleibenden Schwachstellen vorzunehmen. Durch die Bedrohungsanalyse als Ausgangspunkt wurden alle

vorhandenen Gefahren aufgezeigt. Da ein Risiko nur dann vorliegt, wenn Bedrohung und Schwachstelle aufeinander treffen, sollen bei der Schwachstellenanalyse alle die Bedrohungen zusammengefasst werden, bei denen durch Maßnahmen Schwachstellen beseitigt werden können.



VAN ACKEN

Checkliste Risikoanalyse

| Schwachstelle /Risiko | Primäres Schadens-Potential in DEM | Sekundäres Schadenspot. Auswirkung auf das Kerngeschäft in DEM | Schutz-maßnahme | Einmalige Kosten der Schutzmaßnahme in DEM | Laufende Kosten der Schutzmaßnahme in DEM |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |

Schwachstellen-Beseitigung

| Schwachstelle/ Risiko | Empfehlung | Fertigstellungstermin | |
|---|---|---|---|
| | | voraussichtlich | tatsächlich |
| | | | |
| | | | |
| | | | |



**Abbildung 16: Checkliste Risikoanalyse / Schwachstellen-Beseitigung**

Alle Bedrohungen, denen keine Maßnahme zur Beseitigung der Schwachstelle entgegengesetzt werden kann, bilden zusammengefasst das aktuelle Bedrohungspotential. Mittels unternehmensstrategischer Entscheidungen kann dieses Bedrohungspotential durch Abbau von Maßnahmen herauf- oder durch Umsetzung zusätzlicher Maßnahmen herabgesetzt werden.

Das oben bei der risikoorientierten Prüfung beschriebene Vorgehen stellt sich zusammenfassend wie folgt dar:

Für Ihre Notizen

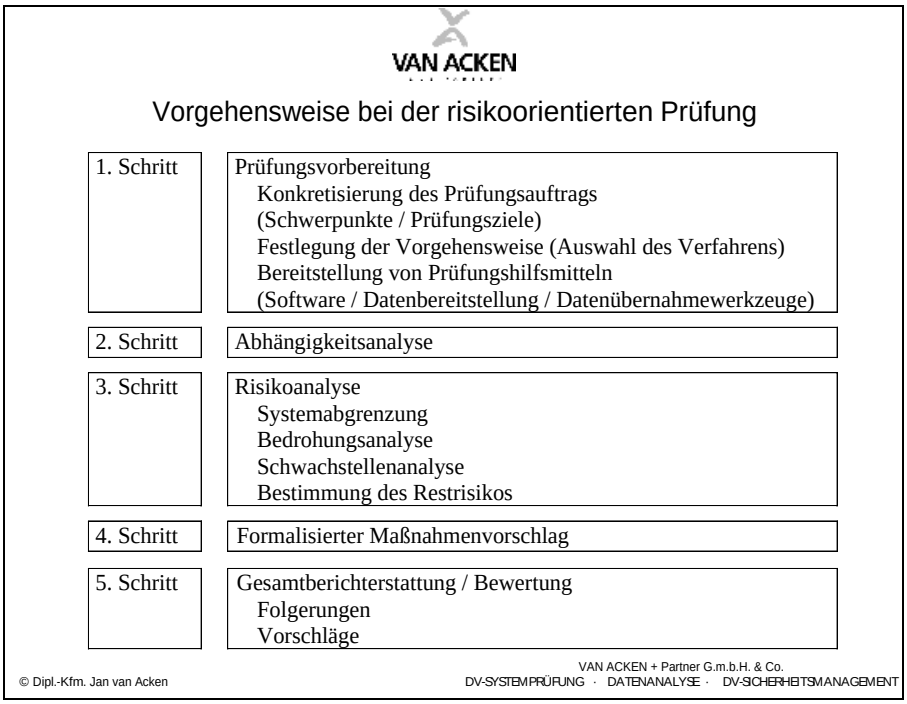



**Abbildung 17: Vorgehensweise bei der risikoorientierten Prüfung**

## Zusammenfassung

Bei den rein nach Risikoaspekten vorgenommenen Prüfungshandlungen, die in direkter Beziehung zur zuvor durchzuführenden Abhängigkeitsanalyse stehen und in einem Maßnahmenvorschlag enden, geht es um das Erkennen aller vorhandenen Risiken, deren Bewertung mit Hilfe der Ergebnisse der Abhängigkeits- und Bedrohungsanalyse und letztendlich um die Bewältigung der aufgezeichneten Risiken anhand ihrer Bewertung.

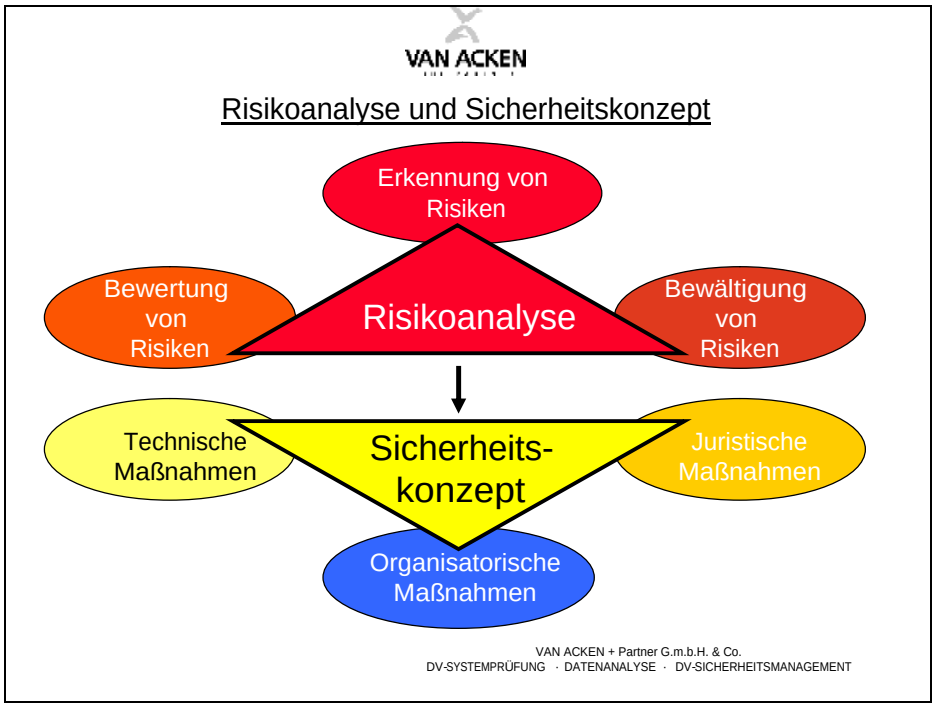



**Abbildung 18: Risikoanalyse und Sicherheitskonzept**[10]

Dieses Vorgehen hat das Ziel, in ein Sicherheitskonzept zu münden, das zunächst einmal einer technischen Umsetzung der vorgeschlagenen Maßnahmen bedarf, flankierend auch zu juristischen Maßnahmen führen kann. Darüber hinaus kann es zu organisatorischen Änderungen kommen unter der Voraussetzung, dass innerhalb der technischen Umsetzung Lücken aufgezeigt wurden. Dies ist eine auch von gesetzgeberischer Seite her zulässige Lösung.

Technisch kann der Revisor beispielsweise durch ein für die Unterstützung genutztes Werkzeug des Bundesamtes für Sicherheit in der Informationstechnik (zukünftig kurz BSI), das IT-Grundschutzhandbuch, unterstützt werden. Hierbei wird eine Verbindung zwischen DV-Systemprüfung und risikoorientierter Betrachtungsweise hergestellt, indem alle vorhandenen DV-technischen Anlagen zunächst erfasst und mit dem ihnen eigenen Risiko bewertet werden. Dann wird mit den innerhalb des Sys-

10 Vgl. Jürgen de Haas und Sixta Zerlauth, DV-Revision, Ordnungsmäßigkeit, Sicherheit und Wirtschaftlichkeit von DV-Systemen, Hrsg. Stefan Fedtke, Anzing, 1999, Seite 46 ff.

Für Ihre Notizen

tems vorliegenden Maßnahmen eine Liste erstellt, die es in der technischen Umsetzung abzuarbeiten gilt. Nach erfolgreicher Umsetzung ist somit ein zuvor festgelegtes Sicherheitsniveau nach dem IT-Grundschutzhandbuch erreicht.

Für Ihre Notizen

## D. Zusammenfassung und Ausblick

Ziel meines Vortrages war es, Ihnen die beiden Vorgehensweisen und Unterschiede der DV-Systemprüfung und des risikoorientierten Ansatzes zu verdeutlichen.

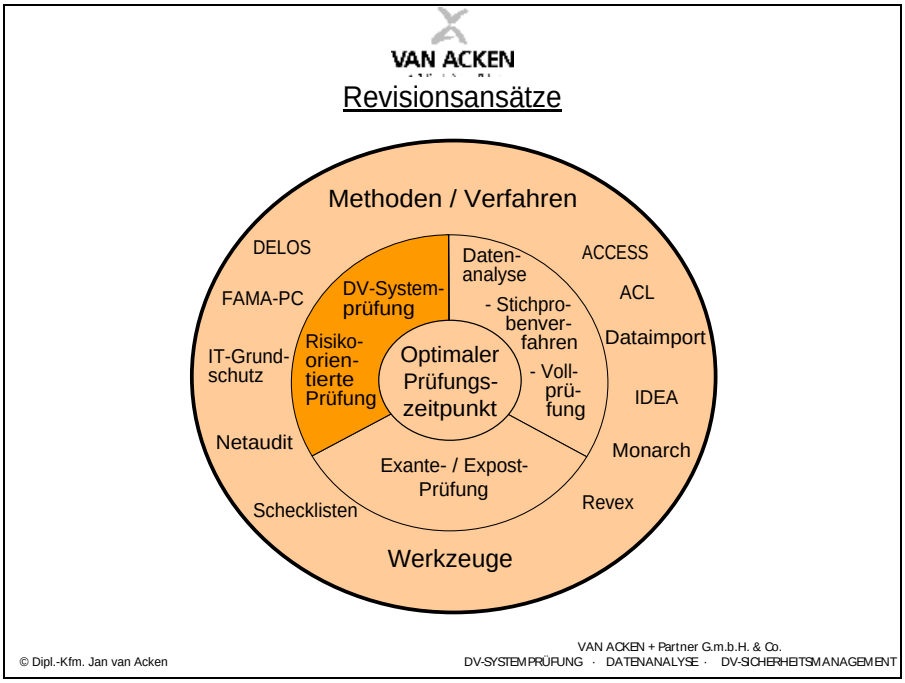



**Abbildung 19: Revisionsansätze**

Bei der Vorstellung beider Verfahren habe ich versucht, mögliche Unterstützungswerkzeuge für beide Vorgehensweisen aufzuzeigen. Die beiden Checklisten-orientierten Systeme, die ausschließlich die DV-Systemprüfung unterstützen, Delos und FAMA-PC, stellen in ihrer Grundausbaustufe eine geringe Hilfe dar. Dagegen bietet FAMA-PC in der Version „Professional“ durch die Möglichkeit zusätzlicher Eintragungen und der Abstimmung der Fragestellung auf das Prüfungsgebiet eine deutlich höhere Unterstützung.

Das am weitesten entwickelte Werkzeug wäre das vom BSI vorgestellte IT-Grundschutzhandbuch, was jedoch im ersten Schritt die Aufnahme aller DV-technischen Komponenten voraussetzt. Hierin ist ein erheblicher zeitlicher Aufwand zu sehen.

Für Ihre Notizen

Bei nochmaliger Betrachtung der die Revision beeinflussenden Faktoren sollte deutlich werden, dass die eben beiden vorgestellten unterschiedlichen Herangehensweisen an DV-Prüfungen auch eine Abhängigkeit zu den gesetzlichen, aber insbesondere den unternehmensinternen Veränderungen darstellen.

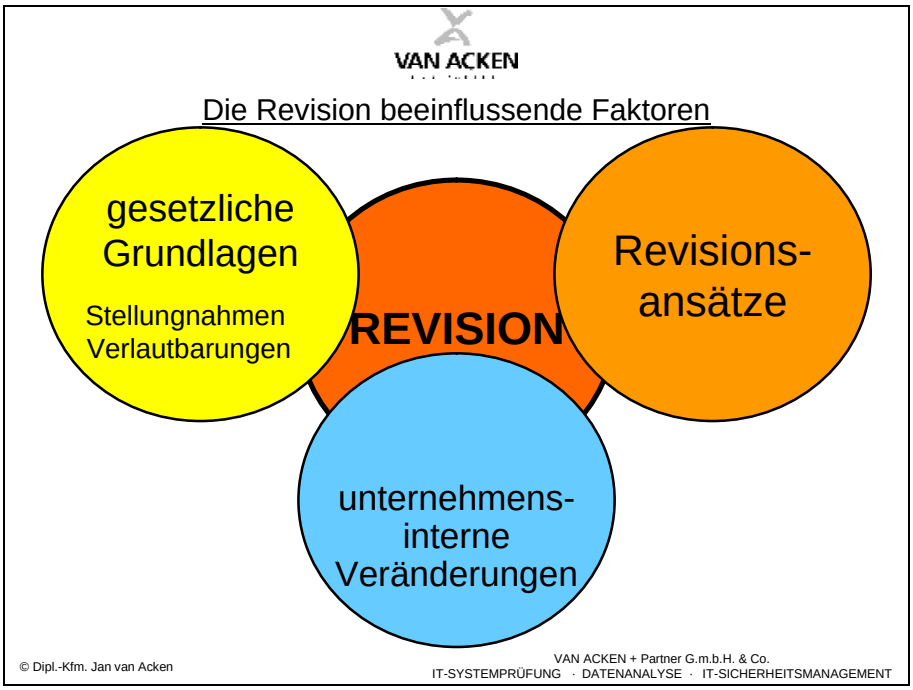



**Abbildung 20: Die Revision beeinflussende Faktoren**

Diese kann beispielhaft dadurch belegt werden, dass der risikoorientierte Prüfungsansatz nach heutiger Kenntnis bei hierarchisch aufgebauten Organisationen höhere Prüfungserfolge verspricht. Bei als Profitcenter geführten Organisationsformen stehen dagegen auf Grund der unterschiedlichen Motivation der Führungskräfte eher Ordnungsmäßigkeitsgesichtspunkte im Vordergrund, weshalb die DV-Systemprüfung einen besseren Ansatz darstellt.

So ist in letzter Zeit innerhalb der Revision auf Grund einer Verlagerung der Organisationsstrukturen der Unternehmen eine Verlagerung auch der Prüfungsansätze festzustellen.

Darüber hinaus sollte deutlich werden, dass auf Grund der sich ändernden Unternehmensstrukturen auch die Prüfungsansätze ggf. geändert werden müssen und eine große Herausforderung

Für Ihre Notizen

der Revisionsleitung darin zu sehen ist, die begrenzten Revisions-Ressourcen so einzuplanen, dass es bezogen auf die Prüfungsobjekte zu einem optimierten der gesamten Organisation zu kommen ist.

Für Ihre Notizen

## I. Abbildungsverzeichnis

## II. Literaturverzeichnis


| | |
|---|---|
| Grebien, Christian | Interne Konzernrevision im Bankbereich, in: Zeitschrift Interne Revision, 34. Jg., Heft 2a, April 1999, Seite 20-28 |
| Haas, Jürgen de und Zerlauth, Sixta | DV-Revision, Ordnungsmäßigkeit, Sicherheit und Wirtschaftlichkeit von DV-Systemen, Hrsg. Stefan Fedtke, Anzing, 1999 |
| Königsmaier, Heinz | Der optimale Prüfzeitpunkt in der Internen Revision – eine Untersuchung des „audit timing-Problems“ aus theoretischer Sicht, in: Zeitschrift Interne Revision 34. Jg., Heft 2a, April 1999, Seite 29-43 |
| Schuppenhauer, Rainer | Grundsätze für eine ordnungsmäßige Datenverarbeitung (GoDV), 4. Aufl., Düsseldorf 1992 |
| Sell, Kirsten | Die Aufdeckung von Bilanzdelikten bei der Abschlußprüfung, Berücksichtigung von Fraud & Error nach deutschen und internationalen Vorschriften, Schriften des Instituts für Revisionswesen der Westfälischen Wilhelms-Universität Münster, hrsg. Jörg Baetge, Düsseldorf, 1999 |
| Stibi, Eva | Prüfungsrisikomodell und Risikoorientierte Abschlußprüfung, IDW-Verlag GmbH, Düsseldorf 1995 |