

Analyseergebnis
aus den in 2005 von REVIDATA durchgeführten
“IT-Prüfungen“

Erkenntnisse, Ergebnisse und Risiken
aus Prüfungen der Informationstechnologie
gemäß IDW PS 330 in der Jahresabschlussprüfung in 2005

- A) IT- Strategie und IT- Wirtschaftlichkeit
- B) IT- Risikobewertung
- C) IT- Organisation
- D) IT- Infrastruktur
- E) IT- Anwendungen
- F) IT- gestützte Prozesse
- G) IT- Überwachungssysteme
- H) IT- Outsourcing
- I) Internetnutzung
- J) Datenschutz
- K) GDPdU

Inhaltsverzeichnis

IT- Strategie und IT- Wirtschaftlichkeit	3
IT- Risikobewertung	3
IT- Organisation.....	3
IT- Infrastruktur.....	4
IT- Anwendungen	4
IT- gestützte Prozesse	5
IT- Überwachungssysteme.....	5
IT- Outsourcing.....	5
Internetnutzung	5
Datenschutz (BDSG).....	6
GDPdU	6

A. IT- Strategie und IT- Wirtschaftlichkeit

Auffällig ist, wie häufig besonders in kleineren und mittleren Unternehmen (KMU), die Planung der Informationstechnologie, sowohl unter technischen aber auch unter wirtschaftlichen Aspekten dem IT-Verantwortlichen überlassen wird. Die Geschäftsführung weiß grundsätzlich was sie an Informationen benötigt, um das Unternehmen führen und steuern zu können, und sie kennt den Grad der Unternehmensabhängigkeit von der Verfügbarkeit der IT. Selten werden diese Themen mit dem IT-Verantwortlichen besprochen. Diesem fehlen somit wichtige unternehmensspezifische Informationen für seine Planung, Umsetzung und den Betrieb. Die Folge davon sind häufig nicht optimale, an die eigentlichen Unternehmensanforderungen angepasste IT- Systeme.

B. IT- Risikobewertung

Als Folge einer häufig fehlenden Kommunikation zwischen der Geschäftsleitung und dem IT-Verantwortlichen werden auch die mit der IT verbundenen Unternehmensrisiken nicht genügend beachtet. Immer wieder weichen die Einschätzungen der erforderlichen IT- Verfügbarkeit von einander ab. Während die Geschäftsführung davon ausgeht, dass bereits nach einer Ausfallzeit von 4- 5 Stunden mit Kunden- und Umsatzverlusten gerechnet werden muss, geht der IT-Verantwortliche in seinen geplanten Maßnahmen von einer Wiederverfügbarkeitsanforderung von ein bis zwei Tagen aus. Vielfach ist selbst diese Planung nicht einzuhalten, da die Vorhaltemaßnahmen nicht vollständig und so gut wie nie getestet werden. Die IT- Verantwortlichen sind selten ausreichend informiert und sensibilisiert und unterschätzen die sich aus einer mangelhaften Betriebssicherheit ergebenden Konsequenzen für das Unternehmen.

C. IT- Organisation

In kleineren und mittleren Unternehmen (KMU) ist die IT- Organisation und die personelle Ausstattung „schlank“ und den Unternehmensmöglichkeiten angepasst. Wie in anderen Unternehmensbereichen ist eine klassische Funktionstrennung und das Vieraugenprinzip wirtschaftlich nicht machbar. Hier ist es zur Vermeidung von Vermögensschäden besonders wichtig in der IT- Abwicklung der Ordnungsmäßigkeit, Nachvollziehbarkeit und Sicherheit große Aufmerksamkeit zu schenken. Leider zeigen unsere Prüfungen, auch zurückzuführen auf das unter A. und B. festgestellte, große Versäumnisse auf, die immer wieder auch den Nährboden für dolose Handlungen bieten. Leider nutzen teilweise gerade die langjährigen Mitarbeiter ihre Erfahrung, den Vertrauensbonus und ihr umfassendes Unternehmenswissen unter dem Druck der heutigen Zeit, zum Schaden der Unternehmen aus.

D. IT- Infrastruktur

Regelmäßig zeigen sich Schwächen und Nachlässigkeiten bei der Beachtung und Einhaltung der einfachsten physischen Sicherheitsmaßnahmen. Vielfach wird der Serverraum als Lager für Papier, Altgeräte und Möbel und selbst als Kaffeeküche und Raucherzimmer genutzt. Es ist überwiegend die fehlende Sensibilität der IT-Verantwortlichen für Risiken und Gefahren, die ein Unternehmen gefährden können. Die gleiche Lässigkeit ist auch im Umgang mit der Datensicherheit, der Datensicherung und der Datenaufbewahrung zu erkennen. Brand-, Einbruch- und Vandalismusgefahr besteht in ihrem Denken nur bei anderen, aber niemals im eigenen Unternehmen. Sie fühlen sich auf einer Insel der Geborgenheit. Über die möglichen Folgen für das Unternehmen machen sich die wenigsten Gedanken und damit auch nicht über die einfachsten Vorbeuge- und Sicherheitsmaßnahmen. Die gesetzlichen Anforderungen des Datenschutzes werden überwiegend genauso wenig beachtet wie die gesetzlichen Aufbewahrungsfristen. Die für das Unternehmen damit verbundenen direkten finanziellen Risiken werden nicht beachtet, da in der Regel nicht bekannt. Das alles zu vermeiden d.h. den Risiken vorzubeugen ist keine Hexerei und kostet nicht viel Geld, auf jeden Fall um ein Vielfaches weniger als ein jederzeit möglicher Schadensfall. Darüber hinaus existiert überwiegend kein Notfallkonzept mit Wiederanlaufverfahren zur Sicherung der Betriebsdaten und der Betriebsbereitschaft.

E. IT- Anwendungen

Selten sind die Anwendungen dokumentiert und damit schwer nachvollziehbar. Handelt es sich um eigen entwickelte Systeme steckt das gesamte Wissen oft in dem Kopf eines einzelnen. Auch die Sicherheit und Richtigkeit der Programme ist nicht sichergestellt. Möglichen Manipulationen ist jeglicher Freiraum gegeben. Dazu kommt die latente Abhängigkeit von dem Entwickler. Mehr und mehr der geprüften Unternehmen entschließen sich zum Einsatz von Standardsoftware. Es wird auch darauf geachtet, dass eine Softwarebescheinigung vorgelegt werden kann. Die Standardsoftware wird auch überwiegend nicht verändert. Vor diesem Schritt werden eher die Geschäftsprozesse angepasst. Sobald es aber zu Anpassungen kommt wird auch bei Fremdlieferanten die Dokumentation zum Teil vernachlässigt, obwohl sie eigentlich zum Lieferumfang gehört. Das liegt wieder an der eigenen Einstellung zur Ordnungsmäßigkeit der Datenverarbeitung die oft fehlt. Besonders auffällig ist die zu erkennenden Nachlässigkeiten in den Schnittstellenbetrachtungen. Selten ist der Datenfluss eines rechnungslegungsrelevanten Datensatzes von der Entstehung über die Schnittstellen zur Buchhaltung abstimmbare und nachvollziehbar. Erschwerend kommt sehr oft hinzu, dass die Datensätze in bestimmten Schnittstellen verändert, manipuliert und auch entfernt werden können. Es gibt selten Schnittstellenprotokolle mit Abstimmsummen und automatischer und vollständiger Protokollierung der Veränderungen. Die Ordnungsmäßigkeit, Vollständigkeit, Richtigkeit und Aktualität der Buchhaltung ist häufig nicht gewährleistet, dass, wenn der Abschlussprüfer dies erkennen würde, er kein, und wenn überhaupt, uneingeschränktes Testet geben könnte. Wirklich wissen kann er es aber nur durch eine fach- und sachgerechte IT-Prüfung mit deren Möglichkeiten des Nachvollzuges. Leider werden wegen dem immer enger werdend Abschlussprüfungsbudget oft nicht die erforderlichen IT-Prüfungen durchgeführt, sondern, wenn überhaupt, lediglich die so genannten "Quick und dirty" Prüfungen. Bei diesen Prüfungen kann die Ordnungsmäßigkeit der Informationstechnologie nicht festgestellt werden.

F. IT- gestützte Prozesse

Was bereits unter dem Punkt E. festgestellt wurde, liegt sehr oft keine Systemdokumentation vor, wodurch auch die IT-gestützten Geschäftsprozesse nur mit hohem Zeitaufwand sachkundig nachvollzogen und geprüft werden können. Hierin liegt ein hohes Risikopotenzial. Unsere im gleichen Zeitraum durchgeführten Zertifizierungen von Standardsoftware hat gezeigt, dass bei bereits auf dem Markt befindlichen Programmen, in bestimmten Konstellationen unserer Tests, Buchungen verloren gehen konnten. Besonders schwierig gestaltet sich oft die Prüfung der Prozesse des Auftragsdurchlaufes bis zur ordnungsgemäßen und vollständigen Verbuchung, ohne eine entsprechende Dokumentation. Auch hier wurden erhebliche Mängel, bis hin zu Umsatzverlusten, festgestellt.

G. IT- Überwachungssysteme

Die etablierten Kontrollen waren überwiegend ausreichend. Sie genügten den betrieblichen Anforderungen weitgehend. Das technische Verständnis war allgemein vorhanden. Eine Interne Revision gibt es in den KMU nicht. Die IT- Leitung übernahm die Kontrollfunktion und informiert die Geschäftsleitung. Die Wirksamkeit der Kontrollen waren meist auf den techn. Betrieb begrenzt. Eine IT- Prüfung durch den Wirtschaftsprüfer war die einzige umfassende Kontrolle und zeigte einige Schachstellen auf.

H. IT- Outsourcing

Zu diesem Prüfungsfeld fanden unsere Prüfer keinen Fall von Outsourcing der Hardware vor. Häufig war die Programmentwicklung und Pflege outgesourct. Neben verschiedenen Standardprogrammen waren firmenspezifische Entwicklungen nach draußen vergeben, um den eigenen Personalbestand den normalen Bedürfnissen entsprechend gering zu halten. Die mit den Softwarelieferanten geschlossenen Verträge waren zum Teil nicht optimal, sondern durch langjährige Bekanntschaft oft zu freundlich gehalten. Die Entwicklung und der Entwicklungsprozess entsprach nicht den heutigen Standards und war damit nicht Qualität gesichert. Eine ordnungsgemäße und nachvollziehbare Dokumentation wurde weder erstellt, noch gehörte sie zum Lieferumfang. Den wenigsten kleineren und mittleren Softwareunternehmen ist geläufig, dass nicht nur die Buchhaltung sondern auch vorgelagerte Systeme, in denen rechnungslegungsrelevante Daten entstehen, prüfungspflichtig und damit ganz bestimmten Grundsätzen der Ordnungsmäßigkeit und Nachvollziehbarkeit (HGB, AO und den korrespondierenden Fachgutachten) unterliegen. In wenigen Fällen wurde auf die Testierung dieser Systeme geachtet.

I. Internetnutzung

Überwiegend war der Internetzugang in den geprüften Mandaten genügend abgesichert. Eigene Internetserver mit Virenschutz, Firewall und Zugriffskontrollen sicherten die Infrastruktur ab. Bei einer Internet gestützten Geschäftstätigkeit wird die erhöht notwendige Betriebsbereitschaft nicht immer genügend beachtet.

J. Datenschutz (BDSG)

Das Bundesdatenschutzgesetz wurde in den geprüften KMU selten, eher nicht, beachtet. Ab einer bestimmten Anzahl von Personen die mit personenbezogenen Daten umgehen, muss es unbedingt Beachtung finden. Erkannte Verstöße können empfindliche Strafen zur Folge haben. Nicht berücksichtigt bei der Bestimmung der Personenzahl, wurden die Anzahl der im Vertrieb und in der Kundenbetreuung eingesetzten Mitarbeiter. Diese personenbezogenen Daten unterliegen aber ebenfalls dem BDSG, sobald mehr als der reine Firmenname gespeichert ist.

K. GDPdU

In unseren Prüfungen haben wir festgestellt, dass die wenigsten Unternehmen genau wissen welche Recht die Finanzverwaltung hat, um digital auf die prüfungsrelevanten Daten zuzugreifen und wie sie vorzubereiten sind. Selbst wenn ein Prüferarbeitsplatz vorhanden war, konnten die erforderlichen Daten oft nicht in der geforderten Form zur Verfügung gestellt werden. Es bedarf einer gründlichen Vorbereitung auch Vorjahresdaten bereit zu halten, besonders wenn zwischenzeitlich ein Systemwechsel stattgefunden hatte. In Dateien von marktgängigen Standardprogrammen waren Sonderzeichen vorhanden die eine normale Verarbeitung mit Prüfungstools nicht zuließen und einen erheblichen Überarbeitungs- und Vorbereitungsaufwand verursachten.