goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

Internes Kontroll-System IKS

Auf den 1. Januar 2008 wurde die Gesetzgebung geändert. IKS erhielt eine gewichtigere Bedeutung. Was bedeutet das für kleinere und mittlere Unternehmungen? Gibt es einen Einfluss auf die IT aus dem IKS oder beeinflusst die IT gar das IKS? Der vorliegende INFONEWS soll diese und weitere Fragen klären. Dabei wird insbesondere auf den Zusammenhang zwischen IKS und IT eingegangen.

Inhaltsverzeichnis

1 DEFINITION IKS 2
1.1 Gesetz 2
1.2 Wer ist davon betroffen? 2
1.3 Was bedeutet interne Kontrolle? 2
1.4 Was ist interne Kontrolle? 3
1.5 Wie gestalten sich die Verantwortlichkeiten? 4
1.6 Wie und in welchem Umfang muss IKS gemacht werden. 4
1.7 Konsequenzen bei fehlendem oder mangelhaftem IKS 4
2 ZUSAMMENHANG RISIKOMANAGEMENT / IKS 5
3 EINFLUSS DER IT AUF DAS RISIKOMANAGEMENT 5
3.1 Beispiel 1: Kino 5
3.2 Beispiel 2: Autoreparaturwerkstatt 7
3.3 Identifikation der Risiken in der IT-Infrastruktur 7
4 KONTROLLE DER IT-INFRASTRUKTUR 9
4.1 Voraussetzungen 10
5 ZUSAMMENFASSUNG 10

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

1 Definition IKS

1.1 Gesetz

Das Gesetz insbesondere das OR (Obligationenrecht) wurde auf den ersten Januar 2008 angepasst. Im Artikel 728 sind folgende Aussagen zum IKS definiert:

Artikel 728a (OR)

- Die Revisionsstelle prüft, ob ein internes Kontrollsystem existiert.
- Die Revisionsstelle berücksichtigt bei der Durchführung und bei der Festlegung des Umfanges der Prüfung das interne Kontrollsystem

Quelle: www.admin.ch

Artikel 728b

- Die Revisionsstelle erstattet dem Verwaltungsrat einen umfassenden Bericht mit Feststellungen über die Rechnungslegung, das interne Kontrollsystem sowie die Durchführung und das Ergebnis der Revision

Quelle: www.admin.ch

Auffällig erscheint, dass in den zitierten Gesetzestexten nie davon die Rede ist, dass ein IKS geführt werden muss. In keinem Artikel des Gesetzes ist einer direkten Form vorgeschrieben, ein IKS zu führen. Aber durch die Formulierung, dass die Revisionsstelle Bericht mit Feststellungen über das IKS erstatten muss, wird ein solches indirekt vorgeschrieben. Ein Internes Kontroll-System zu führen ist folglich eine Pflicht und nicht freiwillig.

1.2 Wer ist davon betroffen?

Betroffen von den im vorhergehenden Abschnitt zitierten Gesetzestexten und damit von der Pflicht ein IKS zu betreiben, sind zwei Arten von Unternehmungen. Einerseits sind dies Publikumgesellschaften, welche der ordentlichen Revision unterstehen. Dazu gehören natürlich Aktiengesellschaften, aber auch beispielsweise die in der Schweiz häufig angewandte Gesellschaftsform der GmbH. Weiter gilt die Regelung aber auch für sogenannte „wirtschaftlich bedeutende Unternehmen“. Der Begriff ist ebenfalls genau definiert. Damit eine Firma zu einem „wirtschaftlich bedeutenden Unternehmen“ wird, müssen zwei der drei folgenden Kriterien in zwei aufeinanderfolgenden Jahren erfüllt werden:

- Bilanz ≥ 10 Mio. Schweizer Franken
- Umsatz ≥ 20 Mio. Schweizer Franken
- Mitarbeiter ≥ 50 Vollzeitstellen im Durchschnitt

1.3 Was bedeutet interne Kontrolle?

Ein internes Kontrollsystem (IKS) besteht aus systematisch gestalteten, organisatorischen Massnahmen und Kontrollen im Unternehmen zur Einhaltung von Richtlinien und zur Abwehr von Schäden, die durch das eigene Personal oder böswillige Dritte verursacht werden können.

Diese zwar etwas langatmige, aber durchaus korrekte Definition von IKS stammt von Wikipedia. Sie sagt eigentlich nichts anderes aus, als dass mit einem internen Kontrollsystem Instrumente geschaffen werden, welche zur Kontrolle und zur Steuerung des Unternehmens auf dem Weg zum Soll-Zustand dienen sollen. Durch die früh-

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

zeitige Erkennung von Kursabweichungen wird es der Geschäftsleitung auch ermöglicht, die entsprechenden Störfaktoren zu identifizieren und die entsprechenden Massnahmen einzuleiten.

Die folgende Grafik soll die Definition der internen Kontrolle noch einmal veranschaulichen.

1.4 Was ist interne Kontrolle?

- Instrumente zur Kontrolle und Steuerung des Unternehmens auf dem Weg zum Soll-Zustand schaffen.



- Die geschaffenen Instrumente nutzen, um Kursabweichungen zu detektieren und die nötigen Massnahmen einzuleiten.



Es stellt sich nun natürlich die Frage, wie können und sollen oder müssen nun diese Instrumente zur Kontrolle des eigenen Unternehmens aussehen. Als erstes gilt es zu vermerken, dass vom Gesetz keine Vorschriften über das „Wie“ gemacht werden. Es genügt allerdings nicht, am ersten des Monats die Liquidität zu prüfen. Die Massnahmen werden auf technischen, wie auch auf organisatorischen Prinzipien aufgebaut. Sie umfassen zum Beispiel:

- Bauliche und Softwaretechnische Zutrittskontrollen
- Schriftliche Weisungen
- Massnahmen zum Schutz der materiellen und immateriellen Vermögenswerte des Unternehmens
- Massnahmen zur Abwehr von illegalen Vorgängen im Bereich Wirtschaftskriminalität

Um geeignete Massnahmen und Kontrollmechanismen zu definieren, ist es unumgänglich, zuerst die angestrebten Ziele zu definieren. Je nach Unternehmen, und insbesondere Unternehmensrisiken, weichen diese voneinander ab. Sie können aber beispielsweise folgende Punkte umfassen:

- Sicherstellung des Normalbetriebs
- Aktiver Schutz vor Notfallsituationen
- Sichern von Betriebsgeheimnissen
- Einhaltung des Soll-Zustandes
- Aktiver Schutz vor Wirtschaftsspionage
- Aktiver Schutz vor Sabotage
- Risikobeurteilung und Berichterstattung
- Sicherstellung, dass die geltenden Gesetze eingehalten werden.
- …

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

1.5 Wie gestalten sich die Verantwortlichkeiten?

Die Verantwortlichkeiten für das interne Kontroll-System sind auf drei Stellen verteilt. Der Verwaltungsrat trägt die Hauptverantwortung. Er entscheidet als erstes darüber, ob ein IKS eingeführt werden muss. Diese Frage sollte sich allerdings erübrigen, da eine Gesellschaft mit einem Verwaltungsrat ja immer dazu verpflichtet ist, ein Internes Kontroll-System zu führen. Allerdings trägt der Verwaltungsrat dadurch auch die Verantwortung darüber, dass ein IKS vorhanden ist. Dem Verwaltungsrat obliegt es weiter, im Bilanzanhang Angaben über die Durchführung einer Risikobeurteilung zu machen. Auch hier handelt es sich um eine Pflicht. Im Verlaufe des Dokumentes wird noch weiter auf diese Risikobeurteilung eingegangen.

Entscheidet der Verwaltungsrat ein IKS einzuführen, muss die Geschäftsleitung mit der Umsetzung beauftragt werden. Diese erhält die Kompetenzen und die Verantwortung darüber. Diese Verantwortung über die Umsetzung kann von der Geschäftsleitung nicht abgegeben oder delegiert werden. Die Umsetzung selbst kann selbstverständlich delegiert werden. Ebenfalls in die Verantwortung der Geschäftsleitung fällt auch das Management der Risiken und Compliance. Auch auf diese Verantwortlichkeit wird noch weiter eingegangen.

Der Revisionsstelle fallen die am klarsten und genauesten definierten Aufgaben und Verantwortlichkeiten im IKS zu. Diese hat, wie im Gesetze festgehalten, zu prüfen ob ein IKS existiert und liefert des Weiteren einen umfassenden Bericht mit Feststellungen zum IKS.

1.6 Wie und in welchem Umfang muss IKS gemacht werden.

Der Gesetzgeber lässt bewusst offen, wie das IKS aufgebaut werden muss. Damit soll den Firmen der nötige Handlungsspielraum gegeben werden, das IKS auf die Unternehmung anzupassen. Die individuellen Gegebenheiten können und sollen berücksichtigt werden. Folgende Kriterien helfen bei der Wahl der Instrumente:

- Grösse
- Komplexität der Geschäftstätigkeit
- Art der Finanzierung

Sehr wichtig ist, dass ein IKS überprüfbar ist. Eine Dokumentation desselben wird damit unumgänglich. Wird das IKS nicht dokumentiert, kann es von der Revisionsstelle auch nicht im gewünschten Umfang kontrolliert werden. Dies hat zur Folge, dass im Bericht der Revision das IKS als ungenügend deklariert werden muss. Interne Kontrolle ist Chefsache. Es gilt aber die Mitarbeiter über dieses, in einer sinnvollen Form, zu informieren (zumindest über einzelne Punkte). Die Information ist zwar nicht vorgeschrieben, untermauert aber eine offene Kommunikationspolitik.

1.7 Konsequenzen bei fehlendem oder mangelhaftem IKS

Wie bereits erwähnt, sind die Revisoren per Gesetz dazu verpflichtet, Ausführungen über das interne Kontrollsystem in ihrem Revisionsbericht an die Generalversammlung zu tätigen. Dort wird natürlich auch festgehalten, wenn ein IKS mangelhaft (z.B. nicht dokumentiert) ist oder komplett fehlt. Die Revisoren müssen

weitere Ausführungen über die Feststellungen im Erläuterungsbericht an den Verwaltungsrat vornehmen. Damit hat der Verwaltungsrat die Möglichkeit festzustellen, wenn die Geschäftsleitung ihre Verantwortung für die Umsetzung des IKS nicht oder mangelhaft wahrnimmt.

Im Falle von ungenügendem IKS wird bei den Konsequenzen unterschieden, ob fahrlässig oder nicht fahrlässig gehandelt wurde. Verletzt ein Organ der Gesellschaft seine Pflichten fahrlässig oder absichtlich, haftet dieses für allfälligen Schadenersatz. Bei weitreichenden Folgen machen sich die Fehlbaren strafbar und können gemäss Strafgesetzbuch Artikel 102 (Organisationsverschulden) belangt werden.

2 Zusammenhang Risikomanagement / IKS

Um das Kontroll-System zu definieren, müssen die Risiken möglichst genau definiert sein. Etwas zu kontrollieren und steuern, das kaum Einfluss auf die Zielerreichung hat, macht üblicherweise wenig Sinn. Sind aber die Risiken identifiziert, können die Kontrollmechanismen genau darauf abgerichtet werden. Eine Risikobeurteilung wiederum ist ein Teilaspekt eines umfassenden Risikomanagement. Der direkte Zusammenhang zwischen dem internen Kontroll-System und des Risikomanagements ist damit direkt gegeben in dem das erstgenannte vom anderen abhängt.

Risikomanagement ist also die Grundlage für ein effizientes Kontroll-System. Das Gesetz schreibt des Weiteren vor, dass jedes Unternehmen eine Risikobeurteilung durchführen muss. Festgehalten ist dies im Artikel 633b Ziff. 12 des Obligationenrechts zum Thema Erfolgsrechnung. Der Anhang enthält Angaben über die Durchführung einer Risikobeurteilung.

3 Einfluss der IT auf das Risikomanagement

Der erste Schritt des Risikomanagements ist die Identifizierung der Risiken. Die folgende Grafik zeigt, dass die IT grosse Einflüsse auf die meisten Risiken direkt oder indirekt hat. Auch wenn die Risiken nicht technisch betrachtet werden. Die gelben Pfeile stellen Risiken dar, auf welche die IT einen indirekten Einfluss hat. Die grünen Pfeile markieren Risiken, auf welche die IT direkten Einfluss hat. Die einzelnen Positionen werden an dieser Stelle nicht weiter kommentiert.

3.1 Beispiel 1: Kino

Anhand eines Beispiels wird an dieser Stellen noch einmal verdeutlicht, dass der Einfluss der IT auf geschäftskritische Prozesse meist sehr gross ist.

Einer der wichtigsten Prozesse eines Kinos stellt die Sitzplatzreservation dar. Ohne Sitzplatzreservation kommen keine (oder nur wenige) Kunden. Der Prozess wird hier in der folgenden Grafik stark vereinfacht dargestellt.

Nun können einerseits direkt involvierte und andererseits indirekt involvierte Systeme unterschieden werden. Als direkt involviert kann logischerweise der Webserver bezeichnet werden. Auch wenn dieser bei einer Hostingfir-

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

ma betrieben wird, darf er nicht einfach aus dem Risikomanagement gestrichen werden. Ebenfalls direkt involviert sind der Datenbankserver sowie der E-Mail-Server, ohne den keine Bestätigung versendet werden kann.

Neben den direkt involvierten Systemen kommen noch die indirekt involvierten dazu. Namentlich gehören eigentlich alle Grunddienste im betroffenen Netzwerk dazu. Ohne diese nützt auch ein korrekt konfigurierter und funktionierender Datenbank-Server wenig.

Zu diesen Diensten zählen unter anderem das Netzwerk ganz allgemein, Firewall / Router, DNS-Server, und die Internetanbindung.

Eine funktionierende IT-Infrastruktur ist folglich wichtige Grundlage für einen fehlerfreien Ablauf dieses, für ein Kino, essentiellen Prozesses. Ähnlich sieht es auch aus, wenn die Reservationen über das Telefon getätigt werden.

3.2 Beispiel 2: Autoreparaturwerk-statt

Bei einer Autoreparaturwerkstatt ist die Kundenauftragsabwicklung ein wichtiger Prozess, wenn nicht sogar der wichtigste. Bei kleinen Werkstätten ist es meist möglich auf Papier zu arbeiten, bei grösseren Betrieben wird aber der Ablauf ohne IT kaum oder nur stark eingeschränkt möglich sein.

In diesem Fall sind die direkt involvierten Systeme der E-Mail-Server, die Auftragsabwicklung, die Bestell-Applikation und die Buchhaltungssoftware. Ähnliche Systeme wie beim Beispiel 1 können auch in diesem Fall als indirekt involvierte detektiert werden. Dazu gehören sicherlich das Netzwerk, die Internet-Anbindung, die Firewall / Router, der DHCP-Server usw.

Obwohl es sich um zwei unterschiedliche Branchen handelt, ist ersichtlich, dass die IT grossen Einfluss auf die geschäftskritischen Prozesse ausübt. Deshalb sollte die IT beim Risikomanagement immer direkt miteinbezogen werden.

3.3 Identifikation der Risiken in der IT-Infrastruktur

3.3.1 Verfügbarkeit

Anhand eines fiktiven Beispiels wird an dieser Stellen aufgezeigt, wie die kritischen Systeme in einer IT-Infrastruktur anhand der Geschäftsprozesse identifiziert werden können. In diesem Abschnitt gilt es insbesondere die kritischen Systeme im Bereich Verfügbarkeit zu finden. Am einfachsten wird dazu eine Verfügbarkeitsmatrix mit den Geschäftsprozessen ausgearbeitet. In der folgenden Grafik sind die Prozesse mit Farben nach deren Wichtigkeit markiert. Rot bedeutet, dass nur eine kurze Ausfallzeit des Prozesses geduldet werden kann, gelb eine mittlere und grün eine längere Ausfallzeit. Durch die Kreuze wird markiert, welche IT-Systeme in welchen Geschäftsprozessen involviert sind.

Verfügbarkeitsmatrix	Prozess 1	Prozess 2	Prozess 3	Prozess 4	Prozess 5	Prozess 6	Prozess 7
Domainkontroller	X	X	X	X	X	X	X
Exchange-Server	X		X	X	X		
Dateiserver	X	X	X	X	X		X
SQL-Datenbank	X			X	X		
CNC-Maschinen	X	X					X
Internetzugang	X				X		
Zugriff von aussen auf Daten	X			X			
Verbindung zu Standort	X					X	X

Anschliessend können anhand dieser Matrix die Anforderungen bezüglich Verfügbarkeit, abgeleitet aus den Geschäftsprozessen, an diese Systeme gestellt werden.

OBJEKT	VERANTWORTLICHKEIT	VERFÜGBARKEIT TAG/NACHT	TOLERIERBARE AUSFALLDAUER TAG/NACHT	PRIORITÄT
Domain-Kontroller	IT	Sehr hoch / hoch	4 / 6	3
Exchange-Server	IT	Hoch / gering	8 / 10	4
File-Server	IT	Sehr hoch / hoch	4 / 6	2
SQL-Datenbank	IT	Hoch / gering	8 / 10	7
CNC-Maschinen	Techniker	Sehr hoch / hoch	4 / 8	1
Internetzugang	Provider	Gering / sehr gering	8 / 10	8
Zugriff von aussen auf Daten	IT	Hoch / gering	6 / 10	6
Verbindung zu Aussenstandort	Provider	Hoch / gering	4 / 10	5

Selbstverständlich ist dieser Prozess in der Praxis nicht ganz so einfach. Insbesondere, da ein Mittelmass zwischen Verfügbarkeit und Kosten gefunden werden muss. Es ist teilweise sehr teuer die Verfügbarkeit zu erhöhen. Ob sich diese Kosten tatsächlich auszahlen, muss separat betrachtet werden. Zumindest erhält man mit der Methode einen schnellen Überblick und kann aktiv verhindern, dass die Verfügbarkeit von einzelnen Applikationen sehr hoch angesetzt wird, während die Grunddienste eine tiefere Verfügbarkeit aufweisen.

3.3.2 Vertraulichkeit

Eine Datenklassifikation ist in den meisten Fällen unumgänglich, wenn sich eine Firma mit diesem Thema auseinandersetzt. Auch hier geht es darum, die kritischen und schützenswerten Daten zu identifizieren. Durch eine Datenklassifikation ist es einfacher, die Risiken zu ermitteln. Eine einfach Variante (die in einigen, aber bei weitem nicht in allen Fällen ausreicht) sieht folgendermassen aus.

Öffentlich	Vertraulich	Geheim
Die Daten in dieser Kategorie gelten als unproblematisch bezüglich Verfügbarkeit. Dazu gehören beispielsweise öffentliche Preislisten, Produktbeschreibungen usw.	Vertrauliche Daten sind meist nur für den internen Gebrauch gedacht. Dazu gehören. Weisungen, Kundenrabatte usw.	Daten der Kategorie Geheim dürfen die Firma auf keinen Fall verlassen z.B. Patientendaten
Daten der Kategorie Öffentlich dürfen veröffentlich werden.	Durch die Veröffentlichung der Daten entsteht ein gewisser Schaden, das Unternehmen ist aber nicht existenziell bedroht.	Bei Veröffentlichung von Daten der Kategorie Geheim ist das Unternehmen existenziell bedroht.

Die Identifikation der involvierten Systeme kann im ähnlichen Stil wie für die Verfügbarkeit mittels einer Matrix herausgefunden werden. Für den Schutz der Daten genügen aber nicht nur technische Massnahmen. Insbesondere in diesem Bereich ist der Mensch die grösste Schwachstelle und muss entsprechend geschult werden.

3.3.3 Integrität

Durch die Datenintegrität wird sichergestellt, dass vorhandene Daten auch zu einem späteren Zeitpunkt nicht verändert werden können. Als Beispiel kann genannt werden, dass ein geheimes Rezept in der Lebensmittelindustrie nie verändert wird (Integrität) und die Firma nie verlässt (Vertraulichkeit). Die Verfügbarkeit spielt dabei eine eher unbedeutende Rolle. Die Risiken können ähnlich wie bei der Vertraulichkeit über Klassifikationen ermittelt werden. Technisch ist eine korrekte Zugriffsbeschränkung essentiell. Gesichert werden können die Daten auch mittels Hashwerten und digitalen Signaturen.

3.3.4 Klassifikation der Risiken

Die in den oberen Abschnitten identifizierten Risiken können anschliessend wiederum anhand einer Matrix und der Kenntnisse der aktuellen technischen Situation in eine klassische Risikobewertungs-Matrix abgefüllt werden. Die folgende Abbildung zeigt eine einfache Form. Die Grundidee besteht darin, die Eintritts-Wahrscheinlichkeit mit dem Schadenspotential zu multiplizieren und so die Grösse des Risikos zu ermitteln.

			Eintrittswahrscheinlichkeit		
			Wenig Wahr-schein-lich	Wahr-schein lich	Sehr Wahr-schein lich
			1	2	3
Schaden bei Eintritt	Gering	1			
	Mittel	2			
	Schwer	3			

4 Kontrolle der IT-Infrastruktur

In den vorangehenden Abschnitten konnte aufgezeigt werden, wie intensiv viele, teils hochkritische Geschäftsprozesse, von der IT-Infrastruktur abhängen. Ein Einbezug der IT-Infrastruktur in das IKS macht deshalb durchaus Sinn. Eine bewährte Möglichkeit einer unabhängigen Kontrolle besteht darin, eine Sicherheitsüberprüfung von externen Spezialisten durchführen zu lassen. Dabei kann insbesondere darauf geachtet werden, ob die vorhandenen Vorgaben auch eingehalten werden, resp. können. Die Überprüfung kann auf den organisatorischen oder auf den technischen Bereich abgehalten werden. Eine Kombination ist selbstverständlich auch möglich. Um die Effizienz solcher Überprüfungen zu steigern können auch Überprüfungen einzelner Teilbereiche, durchaus ihre Berechtigung haben.

Insbesondere wenn Zugriffe aus dem Internet auf die Infrastruktur möglich sind, können auch sogenannte Penetration Tests gute Kontrollinstrumente darstellen. Penetration Tests können aber auch intern stattfinden Dabei wird der illoyale Mitarbeiter simuliert und es wird versucht an Daten zu gelangen, die nicht zugänglich sein sollten.

Mit den beschriebenen Kontrollmechanismen kontrollieren Sie die Sicherheit und die Einhaltung der Vorgaben für Ihre IT-Systeme.

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

4.1 Voraussetzungen

Als Voraussetzung für eine optimale Steuerung und Kontrolle der IT mittels IKS müssen einige Voraussetzungen erfüllt sein. Unter Umständen bedeutet dies einen gewissen Initialaufwand:

- Unternehmensziele und Strategie definiert
- Geschäftsprozesse definiert
- Kritische Prozesse bekannt
- IT-Strategie definiert
- Risikobeurteilung der Prozesse und dadurch abgeleitet die Anforderungen an die unterschiedlichen IT-Elemente bekannt.

Ein Audit oder ein Penetration Test können aber auch wenn nicht alle Voraussetzungen erfüllt sind, einen grossen Nutzen bringen. Das Resultat stellt eine Standortbestimmung dar und zeigt auf, in welche Richtung weiter gearbeitet werden muss.

5 Zusammenfassung

- Jedes Schweizer Unternehmen ist gesetzlich zu einer Risikobeurteilung verpflichtet und muss darüber berichten.
- Die Risikoanalyse ist Teil eines Risikomanagements.
- Jedes der ordentlichen Revision unterstehende Unternehmen ist zur Führung eines IKS verpflichtet. (Die Revision muss dies prüfen)
- Der Gesetzgeber macht keine Vorschriften über das „Wie“.
- Risikomanagement ist eine Grundlage für ein effizientes IKS
- Die kritischen Geschäftsprozesse sind meist von der IT-Infrastruktur abhängig.
- Steht die IT-Infrastruktur still, stehen die meisten Unternehmen auch still.
- Die IT-Infrastruktur Prüfen ist ein Teil des IKSs