IT-Compliance
Teil 1

Prof. Dr. Günther Hellberg © 2019

Motivation

IT-Compliance

- Welche Regeln und Gesetze sind für die IT wichtig?

- Für die Unternehmen ist es lästig, die vielen Compliance-Anforderungen zu erfüllen. Aber unter Umständen lassen sich auch positive Effekte, also Vorteile damit erzielen.

IT-Compliance

- Compliance im IT-Bereich ist etwas, das jedes Unternehmen anstrebt.
- Viele haben es bereits geschafft, ohne es zu wissen; manche wissen nicht genau, was das eigentlich ist, und engagieren deshalb viele externe Berater, die das Problem lösen sollen.
- Der Begriff "IT-Compliance" ist heute fast immer eingebettet in eine Begriffswolke namens GRC (Governance, Risk and Compliance).
- Selten wird er hinreichend genau definiert und keineswegs immer an das eigene Unternehmen angepasst.

IT-Compliance

- Sowohl die exakte Definition als auch das Customizing sind notwendig.
- Sie bilden die Voraussetzung dafür, überhaupt analytische Maßnahmen einleiten zu können
- Vor allem aber ist es wichtig, um einen dauerhaft wirksamen und verbesserungsfähigen Regelkreis für die IT-Compliance aufzubauen.

IT-Compliance

- Einen IT-Compliance-Officer oder -Beauftragten auszurufen führt allein nicht weiter.
- Ebenso wenig zielführend ist es, allen Normen genügen zu wollen. Und selbstverständlich nutzen die Compliance-Anstrengungen auch nicht viel, wenn nicht alle oder die falschen Bestimmungen eingehalten werden.
- Aber was ist eigentlich IT-Compliance?
- Das wollen wir in diesem Quartal beleuchten und möglichst präzise erarbeiten.

IT-Compliance

- Lassen Sie uns aber vorher auch noch einmal überlegen, welche Argumente wir FÜR IT-Compliance finden können!
- Hierfür ist die Betrachtung der verschiedenen Perspektiven sehr hilfreich.

Argumente für die Chefetage

- **Argumente für die Chefetage**
- Das Budget für Compliance-Projekte können Sie sich auch verschaffen, indem Sie die Vorteile herausstellen:
- Eine effektive IT-Compliance erhöht den Wertbeitrag der IT für das Business.
- Sie hilft, Risiken zu vermeiden und zu minimieren.
- Sie schützt vor konkreten Nachteilen, zum Beispiel Haftung oder Imageverlust.
- Sie steigert die IT-Sicherheit und die IT-Qualität.
- Langfristig verringert sie die IT-Kosten, indem sie die Zentralisierung fördert und Synergien ausschöpft.

Interne IT-Comliance

IT-Compliance

- **Interne IT-Compliance**
- Von IT-Compliance spricht man, wenn alle für die IT einer juristischen Person verbindlich vorgegebenen Regeln und als verbindlich akzeptierten Vorgaben nachweislich eingehalten werden.
- Hierbei gibt es eine externe und eine interne Perspektive der IT-Compliance.

IT-Compliance

- Die interne Compliance betrifft den Regelungskontext, den sich das Unternehmen selbst setzt - für seine Geschäftsprozesse oder deren IT.
- Dabei geht es um interne Vorgaben, mit denen Nachhaltigkeit, Prüfbarkeit und Dokumentation der Informationstechnik gewährleistet werden sollen.
- Diese Vorgaben sind weitestgehend unter den Begriff IT-Governance einzuordnen.
- Wenn beispielsweise die IT-Governance voraussetzt, dass der IT-Betrieb nach Itil und ISO 20000 oder Cobit zu organisieren ist, dann hat sich die IT auf diese Vorgaben einzustellen.
- Sie muss dafür sorgen, dass sich die Erbringung der IT-Services konform zu diesen Regeln verhält.

IT-Compliance

- Aber das ist sozusagen nur die Kür, denn niemand ist rechtlich gezwungen, einen solchen internen Standard zu setzen.
- Es mag allerdings Grenzfälle geben, wo zum Beispiel die Einführung und Einhaltung einer ISO-9000-Norm für ein Management-System nicht ganz freiwillig geschieht, sondern vom Business unter Marktgesichtspunkten als notwendig erachtet wird.
- Häufig soll auch der Nachweis einer erfolgreich testierten BSI-Grundschutzzertifizierung dazu dienen, dem Wirtschaftsprüfer schnellere und kostengünstigere Prüfungsmöglichkeiten zu bieten.

Externe IT-Comliance

IT-Compliance

- **Externe Compliance**
- Viel wichtiger als die Kür ist aber die Pflicht, also die IT-Compliance aus externer Perspektive.
- Gemeint sind hier die Kenntnis und das Einhalten von Vorschriften (Gesetzen, Verordnungen, Rechtssprechung, Verträgen) für die Geschäftsprozesse und IT-Services des jeweiligen Unternehmens.
- Werden sie nicht befolgt, hat das Folgen. Es führt zu überwiegend zivilrechtlichen und zuweilen auch strafrechtlichen Sanktionen für das Unternehmen, dessen Leitung oder die handelnden Personen.

IT-Compliance

- Sowohl aus der externen IT-Compliance-Sicht als auch aus der Perspektive der IT-Governance ist das Risiko-Management zu betrachten.
- Dessen erfolgreiche Umsetzung für die Geschäftsprozesse wird beispielsweise im Bankenumfeld von Basel II oder MA Risk (Mindestanforderungen für das Risiko-Management) vorausgesetzt.
- Bisweilen ist es auch für den IT-Provider selbst gefordert, wenn er eine juristische Person im Unternehmen ist oder im Outsourcing-Kontext handelt.

Die Normen im Überblick

IT-Compliance

- **Die Normen im Überblick**
- Was ist zu tun?
- Der IT-Manager sollte damit beginnen, nach verbindlich vorgegebenen externen Regeln zu suchen.
- Er braucht dafür den Überblick, welche externen Regeln für sein Unternehmen und speziell für dessen IT gelten.
- Diese Analyse kann der IT-Bereich üblicherweise nicht allein vornehmen.

IT-Compliance

- Dringend anzuraten ist die Zusammenarbeit mit dem Unternehmensjuristen und mit Vertretern der Business-Units.
- Wenn es eine unternehmensweite Compliance-Stelle oder einen Beauftragen für das interne Kontrollsystem (IKS) gibt, wird von dort sicher auch Unterstützung zu erwarten sein.
- Die externen Normen lassen sich unterscheiden nach generellen, für alle Unternehmen verbindlichen Vorschriften auf der einen Seite und Regeln, die von der Rechtsform, der Art des Business oder dem Land der Unternehmung abhängen.
- Die folgende Aufstellung "Externe Normen" gibt einen Überblick, der keinen Anspruch auf Vollständigkeit erhebt.

Externe Normen

- **Externe Normen im Überblick**
- 1. Für alle juristischen Personen des privaten Rechts in Deutschland, also Kapitalgesellschaften wie Aktiengesellschaften (AG) und Gesellschaften mit beschränkter Haftung (GmbH), gelten die folgenden Anforderungen:

IT-Compliance

- **a. zur externen Kontrolle** (durch Steuerbehörden und Buchführungssysteme)
- HGB (Handelsgesetzbuch);
- Abgabenordnung;
- gegebenenfalls IFRS/IAS (internationale Rechnungslegung), BilMoG (Bilanzrechtsmodernisierungs-Gesetz);
- GoB und GoBS (Grundsätze ordnungsgemäßer Buchführung/Buchführungssysteme);
- Rundschreiben und Standards des Instituts der deutschen Wirtschaftsprüfer, zum Beispiel IDW FAIT I, II und III;
- GdPDU (digitale Betriebsprüfung);

IT-Compliance

- **b. zur internen Kontrolle** (IKS, eingeführt durch das KonTraG im Jahr 1998)
- Paragraf 91 Absatz 2 des Aktiengesetzes (gilt auch für große GmbHs);
- **c. hinsichtlich des Datenschutzes**
- BDSchG (Datenschutzgesetz) und
- Landes-DSch-Gesetze;
- **d. gemäß Umsatzsteuerrecht**
- Paragraf 14 UStG (Aufbewahrung von Rechnungen);
- **e. nach dem Urheber- und Lizenzrecht**
- UrhG;
- **f. zum Vertrauen im Handelsrecht**
- SigG (Signaturgesetz);
- Ehug (elektronisches Handels- und Genossenschaftsregister).

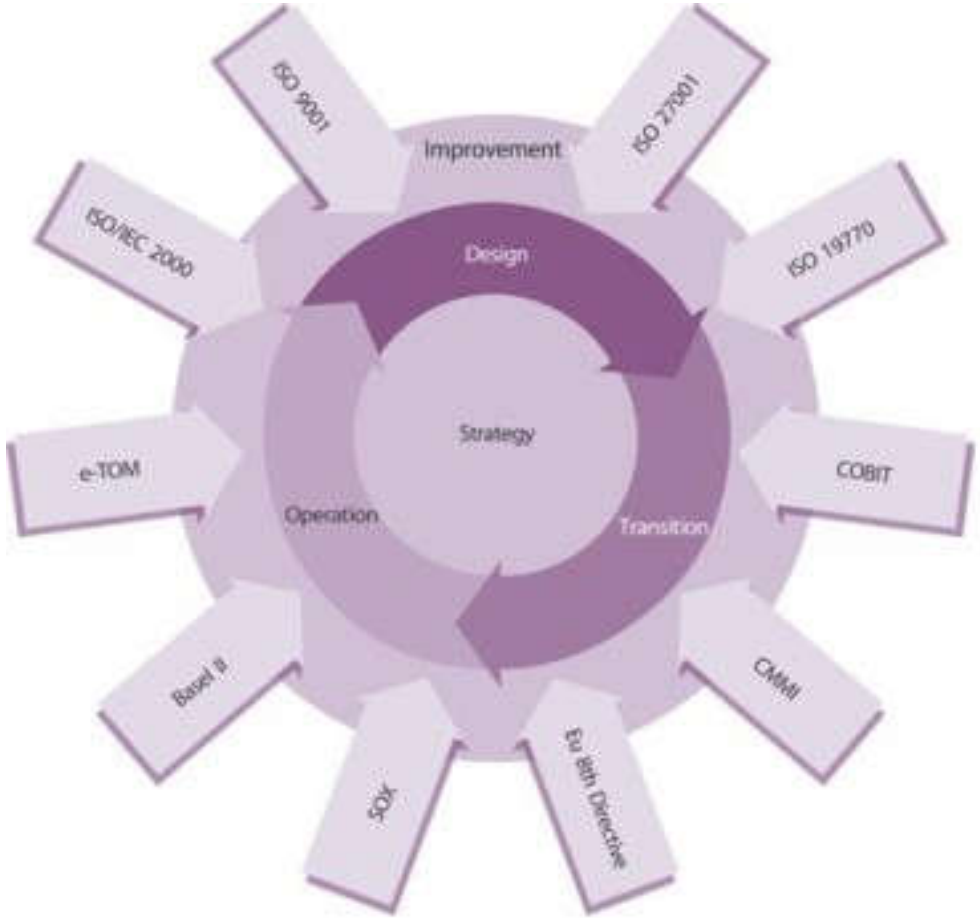
- **b. für Versicherungen**
- Solvency II (Risiko-Management);
- **c. für die Pharma- und Lebensmittelbranche**
- FDA-Regeln (Good Practices) wie GMP, GLP und GCP;
- entsprechendes EU-Recht;
- **d. für Hersteller von Produkten** (Dokumentations- und Beweispflichten, Aufbewahrung)
- Produkthaftungsgesetz.

- **2. Branchenspezifische Regelungen** ergänzen die oben aufgeführten Normen. Dazu zählen beispielsweise:

- **a. für Banken und Kapitalanlagegesellschaft (KAG)**
- KWG (Kreditwesengesetz), KAG (Kapitalanlagegesetz), WpHG (Wertpapierhandelsgesetz);
- Basel II: Gesetz dazu ab 2007 durch das KWG sowie die Solvabilitätsverordnung (SolvVO) umgesetzt;
- BaFin-Regeln (Mindestanforderungen der Bankenaufsicht, zum Beispiel MA Risk);

- **3. Hinzu kommen landesspezifische Regelungen**, zum Beispiel für Unternehmen unter SEC-Aufsicht (an den US-Börsen notiert), etwa
- Sarbanes Oxley Act (Wirtschaftsprüfung).
- **4. Für die öffentliche Verwaltung** gelten besondere Regeln:
- IuK-Mindestanforderungen (Rechnungshöfe);
- Das BSI-Grundschutzhandbuch.

- **Beitrag des Service-Managements**

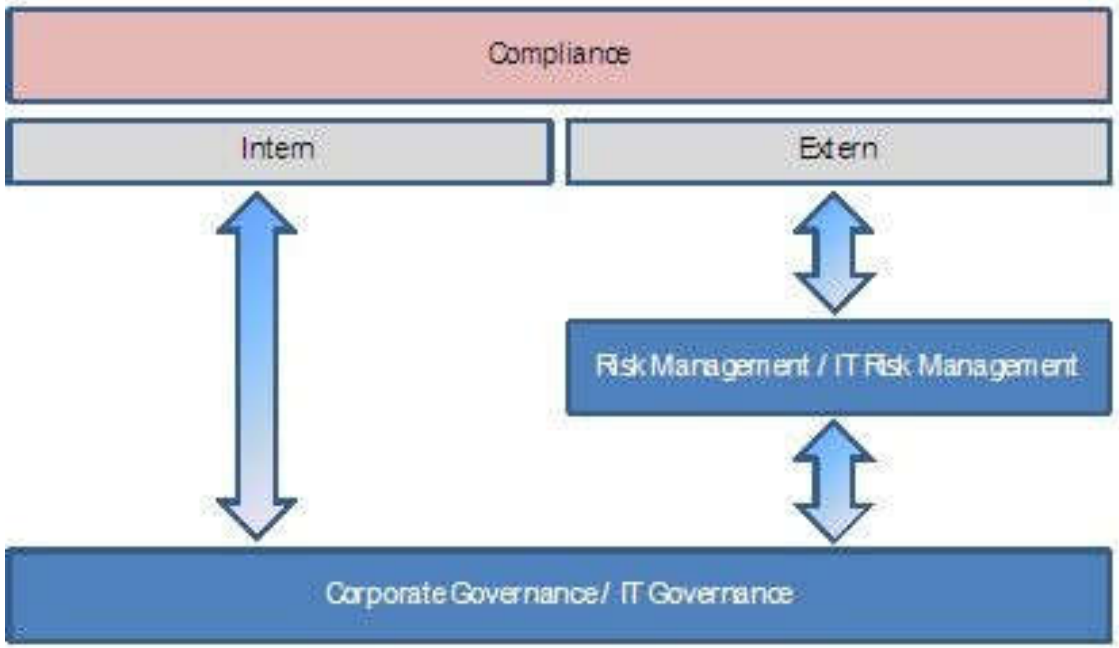


- Auch der IT-Service-Management-Standard Itil geht auf das Thema Compliance ein.

IT-Compliance

- Das Schaubild aus der aktuellen Itil-Version (IT Infrastructure Library) veranschaulicht die Faktoren, die auf das IT-Management und dessen Compliance-Ansätze Einfluss nehmen.
- Dort wird allerdings mehr Wert auf die internen Compliance-Regeln gelegt, die sich das Unternehmen selbst gibt, als auf die externen Regeln, denen es genügen muss.
- Eine IT-Compliance ist immer einzubetten in die IT-Governance-Strukturen des Unternehmens.
- Bei den Zielen und den verwendeten Frameworks gibt es darüber hinaus Synergien zwischen Business- und IT-Prozessen.
- Zudem leistet die IT-Compliance auch einen Beitrag zur Performance des Unternehmens, indem sie Services und deren Wertbeitrag transparent macht.

- Compliance im Unternehmenskontext



(Quelle: Jürgen Dierlamm)

IT-Compliance

- IT-Services sind nicht nur Teil der Compliance-Prüfung, sondern helfen auch kräftig mit, die Compliance einzuhalten beziehungsweise Verstöße aufzudecken.
- Zum Beispiel werden unter dem Stichwort GRC häufig nur Tools aus dem Umfeld des Identity- und Access-Management (IAM) verstanden.
- Doch diese Systeme können durch Role Based Access Control (RBAC) viel zu einer verbesserten Unternehmens-Compliance beitragen (beispielsweise für die Einhaltung des Vier-Augen-Prinzips in der Buchführung).

IT-Compliance

1. Welche Rechtsnormen gelten genau für die IT meines Unternehmens? (Sortieren Sie diese nach Vorschriften für alle Unternehmen sowie dediziert nach Rechtsform, Branche und Ort der Business-Tätigkeit.)

2. Welche Vorgaben, Frameworks und Best Practices (Corporate- und IT-Governance) hat sich mein Unternehmen gesetzt?

3. Welche IT-gestützten Business-Prozesse und übergreifenden IT-Services sind davon betroffen, welche Anforderungen müssen dafür erfüllt sein?

Beispiel für Checkliste

IT-Compliance

- Beispiel für eine **Checkliste** für die Einführung:
- IT-Compliance-Prozesse einzuführen ist eine komplexe Angelegenheit.
- Wer Systematik hineinbringen will, kann sich an folgenden Fragen orientieren:

IT-Compliance

1. Welche Rechtsnormen gelten genau für die IT meines Unternehmens? (Sortieren Sie diese nach Vorschriften für alle Unternehmen sowie dediziert nach Rechtsform, Branche und Ort der Business-Tätigkeit.)

2. Welche Vorgaben, Frameworks und Best Practices (Corporate- und IT-Governance) hat sich mein Unternehmen gesetzt?

3. Welche IT-gestützten Business-Prozesse und übergreifenden IT-Services sind davon betroffen, welche Anforderungen müssen dafür erfüllt sein?

4. Welche Risiken gibt es - mit welchem Schadenspotenzial infolge fehlender oder mangelhafter Compliance?

5. Welche konkreten IT-Compliance-Anforderungen haben die einzelnen IT-Lieferanten (interne und externe Provider sowie technische Bereiche) zu erfüllen (zum Beispiel Active Directory, SAP, Datenbanken oder Netz)?

6. Welche technischen, organisatorischen, personellen und vertraglichen Maßnahmen sind für die dauerhafte Erfüllung der IT-Compliance zu treffen?

7. Wie kann der Erfolg in einem dauerhaften Prozess (ähnlich dem Security-, Risiko-Management- oder IKS-Prozess nach Best Practices) etabliert und abgesichert werden?

8. Welche Schlüsse sind aus einem kontinuierlichen Verbesserungsprozess zu ziehen (Review, Folgemaßnahmen)?

Wenn Sie diese Reihenfolge als grobe Leitlinie für ein IT-Compliance-Projekt und dessen nachfolgende Implementierung in der Linienorganisation berücksichtigen, können Sie so falsch gar nicht liegen.

Fazit / Ausblick

ENDE

Fragen?