

Modernes Informationsmanagement mit Erfüllung aller Compliance Anforderungen.

Wie kann das aussehen? Ein Beispiel mit:

WISDOM Windows und Internet System für Dokumenten-Management
flexibler, individueller, kundenorientierter



Vortrag für DGQ-Regionalkreis Ostwestfalen-Lippe
im Zuge der MEiM 2015 Messe: Mehr Erfolg im Mittelstand, Kundenforum A
am 28.10.2015 in Paderborn

Dipl. Ing. Hans-Werner Wenglorz
Dipl. Inform. Erich Mertins

Agenda

1. Teil:

Was ist Informationsmanagement und welche Compliance-Anforderungen aus Normen, Gesetzen, Vorschriften, Regelungen – intern als auch extern – müssen eingehalten werden? (Wenglorz)

2. Teil:

Das Normen- und Dokumentenverwaltungsprogramm WISDOM wird erklärt und anhand von Praxisbeispielen diese Durchgängigkeit gezeigt, um complianced zu werden und zu bleiben. (Mertins)

Vorstellung der Vortragenden im jeweiligen Teil

Seite 3

Vita Hans-Werner Wenglorz
Jahrgang 1948, Dipl.-Ing. Maschinenbau

- ❖ **1976 - 1990** Reaktorbau Industrie
- ❖ **1990 - 2013** Aluminium Industrie

}

Leitung von

- Zentr. Normung, Qualitätsmanagement,
- Compliance- und Riskmanagement



DGQ-Mitglied seit über 25 Jahren
seit 2008 DQS-Auditor

❖ **Ausgebildet und zertifiziert in den Managementsystemen:**

- Qualität (ISO 9001, ISO/TS 16949, VDA 6.3)
- Umwelt (ISO 14001)
- Risiko (ISO 31000, ONR 49000ff) und
- Normen (DIN zertifizierter Normenexperte);

}

auch als Auditor und
Lead Auditor

Weitere Infos unter:
<http://www.beuth.de/de/autor/hans-werner-wenglorz/autoren:tin21:95497823>

AGU – 2015
Wenglorz – ©

Seite 4

1. Teil

**Was ist Informationsmanagement und
welche Compliance- Anforderungen aus
Gesetzen, Vorschriften, Regelungen, Normen
– intern als auch extern –
müssen eingehalten werden?**

DGQ-Regionalkreis Ostwestfalen-Lippe,
 im Zuge der MEiM 2015 Messe: Mehr Erfolg im Mittelstand, Kundenforum A
 am 28.10.2015 in Paderborn
 Hans-Werner Wenglorz

AGU – 2015
Wenglorz – ©

Gliederung

1. **Begriffserklärung Informationsmanagement**
2. **Zwänge der Unternehmen**
 - 2.1 Zwänge von außen auf die Unternehmen
 - 2.2 Zwänge von Unternehmen nach außen
 - 2.3 Zwänge innerhalb des Unternehmens
3. **Resümee: Unternehmensspezifisches Betroffenheits- / Sicherheitsprofil (Risk-Manual)**
 - 3.1 Die Welle der Informationsflut rollt
 - 3.2 Zwänge durch Norm- / Rechtsforderungen
 - 3.3 Zwänge durch Rechtsforderungen
 - 3.4 Betroffenheits- / Sicherheitsprofil (Risk-Manual) => Einflüsse auf das Produkt
 - 3.5 Informationsmenge – viel zum Lesen
4. **Ausgangsbasis: der moderne Risikobegriff**
5. **Compliance Management**
 - 5.1 Begriffsklärung: Compliance vs. Konformität
 - 5.2 Wofür Compliance Management?
 - 5.3 Warum ist Compliance Management unerlässlich?
 - 5.4 Projekt „gerichts feste Organisation“
 - 5.5 Beispiel von Fragen der (internen) externen Auditoren
 - 5.6 Fazit: Compliance Management ist unerlässlich!
 - 5.7 Programm um complianced zu werden und zu bleiben - Beispiel

1. Begriffserklärung

Informationsmanagement:

- strategisches (Informationsmanagement)
- taktisches (Informationsmanagement)
- **operatives (Informationsmanagement)**
 ...nutzt die vorgegebene Informations-Infrastruktur,
 um die richtigen Informationen am benötigten Ort
 und zum passenden Zeitpunkt bereitzustellen.

2. Zwänge der Unternehmen

Seite 7

2.1 Zwänge von außen auf die Unternehmen

➤ Gesellschaftliche, ökonomische und rechtliche Zwänge

Sicherheit, Umwelt, Compliance, Harmonisierung des Handels und der Märkte

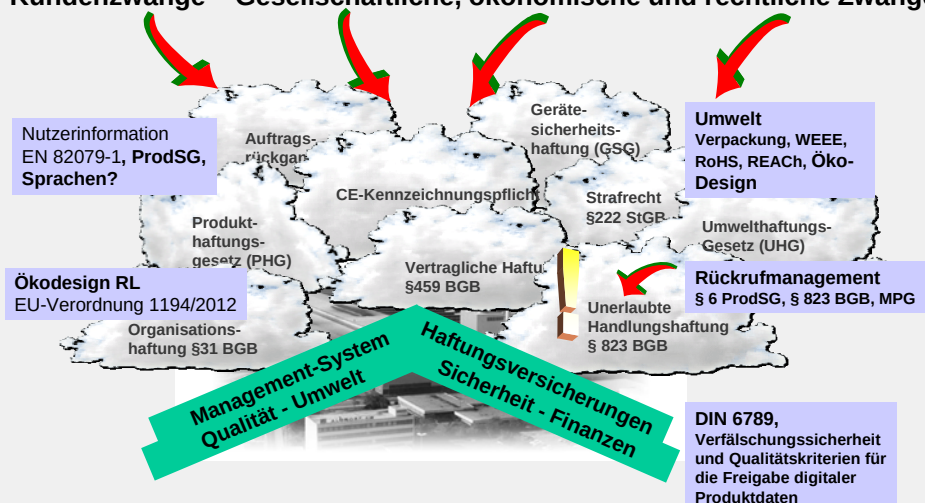
➤ Kundenzwänge

- Qualitäts-/ Umwelt-/ Energiemanagementsystem, etc.
- Harmonisierung der Produkte und deren Komponenten
- Harmonisierung der Dokumentation und deren Informationen
- Harmonisierung der Logistik, etc.

2.1 Zwänge von außen auf die Unternehmen rechtliche und normative Beispiele

Seite 8

Kundenzwänge – Gesellschaftliche, ökonomische und rechtliche Zwänge



2.1 Zwänge von außen auf die Unternehmen

Beispiel: Betriebsorganisationspflicht (§ 823 BGB)

Seite 9

➤ Betriebsorganisationspflicht (§ 823 BGB)

❖ Verkehrssicherungspflicht (wird nach h. M. im objektiven Tatbestand von § 823 Abs. 1 BGB geprüft).

- ✓ Weiterbildung, kompetentes Personal
 - Wissensmanagement (VDI 5610), **neu** in DIN EN ISO 9001:2015 „**das Wissen der Organisation**“ wird als Ressource explizit aufgenommen (Abschnitt 7.1.6): **Die Organisation muss für den Betrieb der Prozesse die erforderlichen Kenntnisse ermitteln um die Konformität von Produkten und Dienstleistungen zu erzielen.**
- ✓ Risikomanagement (ONR 49000ff, ISO 31000, ISO/IEC 31010)
- ✓ Produktbeobachtungspflicht (Rückrufmanagement)
- ✓ Bekanntmachung der jeweils geltenden anerkannten Regeln der Technik sowie **Rechtsvorschriften**
- ✓ Qualitätsmanagement (ISO 9001 „Prozesse“)

AGU – 2015
Wenglorz – ©

2.1 Zwänge von außen auf die Unternehmen

- weltweiter Marktzugang durch Kennzeichnung

Seite 10



AGU – 2015
Wenglorz – ©



Austria	Belgium	Canada*)	Czech Republic a. Slovakia	Denmark
Germany	Finland	France	Great Britain	Hungary
Italy	Netherlands	Norway	People's Republic of China	Poland
Russia	Sweden	Switzerland	Spain	USA*)

- Die bedeutenden Hersteller in Europa lassen ihre Produkte zertifizieren
- Durch Kooperation mit Prüfstellen werden die Zeichen überwacht und haben den vollen Stellenwert

- AGU – 2015
-
- Wenglorz – ©

2.2 Zwänge von Unternehmen nach außen

- **Einflussnahme auf die Gesellschaft und deren gesetzte und normative Festlegungen**
 - Einfluss auf laufende Gesetzesvorgaben, die die Produkte und Produktionsverfahren einschränken würden (Lobbyismus)
 - Einfluss auf laufende Normungsverfahren, die sich auf Produkte und Produktionsverfahren auswirken (Gemeinschaftsarbeit der interessierten Kreise in Normungsgremien)
- **Einflussnahme auf den Markt**
 - Durchsetzung seiner Produkte als Standard
 - Durchsetzung seiner Dokumentation als Standard [z.B. Instandhaltung (ISO 55000, PAS – Asset Management)]
 - Durchsetzung seiner Logistik als Standard
 -

s.a. weltweite Kennzeichnungen, S. 11

2.3 Zwänge innerhalb des Unternehmens

- **Einflussnahme auf eine geregelte Bewirtschaftung und Steuerung von Informationen**
 - Aufbau der Datenbanken und deren Inhalte
 - Steuerung der Informationen im DV-Bereich und auf Unterlagen (z.B. Informationssicherheitsmanagement DIN ISO/IEC 27001)
- **Einsetzung aller Maßnahmen zur Verringerung der Kosten**
 - Senkung von Teilen und Materialien
 - Standardisierung sich wiederholender Vorgänge
 - Regelung von Abläufen - Geschäftsprozessmodellierung und Workflow-Management

2.3 Zwänge innerhalb des Unternehmens Ist-Zustand

Seite 15

- Ungenügende Kenntnisse der Normung der Konstruktions- & Entwicklungsabteilungen (Wenn keine Normenstellen existieren)
- Nicht ausreichende Rechtskenntnisse in allen Bereichen (Selbst Hausjuristen kennen sich im Bereich Produkthaftung/CE-Kennzeichnung nicht aus)
- Eine Ursache ist die nicht ausreichende Ausbildung zu diesen Themen in den Ingenieurwissenschaften

AGU – 2015
Wenglorz – ©

3. Resümee: Unternehmensspezifisches Betroffenheits- / Sicherheitsprofil (Risk-Manual)

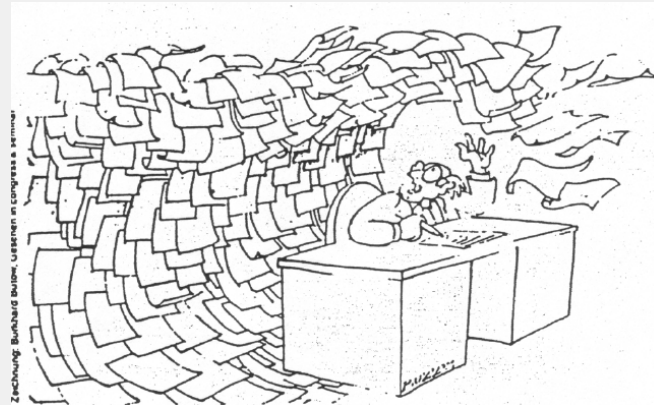
Seite 16



Zusammenfassung der relevanten Normen, Regeln, Richtlinien, Vorschriften u. Gesetze im „Normenwerk“ (Risk-Manual) aufgrund wichtiger externer Einflüsse

AGU – 2015
Wenglorz – ©

3.1 Die Welle der Informationsflut rollt !



 **im Beruf**
 **und privat**

3.2 Zwänge durch Norm- /Rechtsforderungen

Vor dem Hintergrund der Stichworte

➤ Zertifizierung (DIN EN ISO 9001, ISO/TS 16949, VDA 6.1, DIN EN ISO 14001, BS OHSAS 18001 +2 (soll 2016-10 als ISO 45001 erscheinen), DIN EN ISO 22000, ONR 49000ff (ISO 31000), DIN ISO/IEC 27000ff, DIN EN ISO 50001, ISO 19600 und IDW EPS 980 etc.

- Qualitätsmanagement
- Umweltmanagement
- Arbeitssicherheitsmanagement
- Lebensmittelsicherheits-Managementsystem
- Risikoanalyse (Risk-Management)
- Informationssicherheits-Managementsystem
- Energiemanagement Systeme i.V.m. EnEV
- Compliance-Management

hat die Dokumentation, und hier insbesondere die Dokumentation technischer Daten für Produkte, einen besonderen Stellenwert erhalten.

3.2 Zwänge durch Norm- /Rechtsforderungen Übersicht Normen – EG/EU-Richtlinien

Beispiel:

EU-Richtlinie, Verordnung		Daraus resultierende Normen	
Kurztitel	Nummer	Harmonisiert ^{*)}	Mandatiert ^{*)}
Maschinenrichtlinie	2006/42/EG	873	
Niederspannungsrichtlinie	2006/95/EG	1380	
Druckbehälterrichtlinie	2009/105/EG	15	
Druckgeräterichtlinie	2014/68/EU	250	
Produktsicherheitsrichtlinie	2001/95/EG	65	
EMV-Richtlinie	2004/108/EG	237	
Messgeräterichtlinie	2004/22/EG	25	
Medizinprodukterichtlinie	93/42/EWG	288	
Verpackungsabfallrichtlinie	2004/12/EG	15	
		Σ 3148	

Beispiel für Maschinenrichtlinie 2006/42/EG harmonisierte Normen:

http://ec.europa.eu/enterprise/policies/european-standards/harmonised-standards/machinery/index_en.htm

*) harmonisierte und nationale Normen sowie techn. Spezifikationen i.S. Art. 5 Abs. 1 Satz 2 (H + M = Harmonisiert u. Mandatiert, d.h. als harmonisierte Normen im Sinne des neuen Konzepts werden die europäischen Normen angesehen, die europäische Normenorganisationen (CEN; CENELEC; ETSI) der europäischen Kommission formell vorlegen und die in deren Auftrag (Mandat) erarbeitet wurden = mandatierte Norm).

Wenn man davon ausgeht, dass die Summe der mandatierten Normen mindestens genau so hoch sein wird, wie die der harmonisierten, ist die Gesamtsumme aus den o.a. EU-Richtlinien und Verordnungen ca. 6.500 Normen.

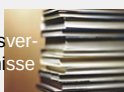
3.3 Zwänge durch Rechtsforderungen

- Compliance bedeutet **Übereinstimmung** mit den Rechtsvorschriften.
- „Regulatory Affairs“ bedeutet „fremde Rechtsordnungen im **globalen Markt**“
- Diese gilt es zu **kennen** und zu **erfüllen**, **bevor** ein Hersteller den Markt betritt
(s. a. 2.1: Produktbeobachtungspflicht / Marktbeobachtung)
- **Ziel:** Vermeidung einer Haftungsinanspruchnahme sowie möglicher Marktzugangssanktionen



Gesetzes-
texte

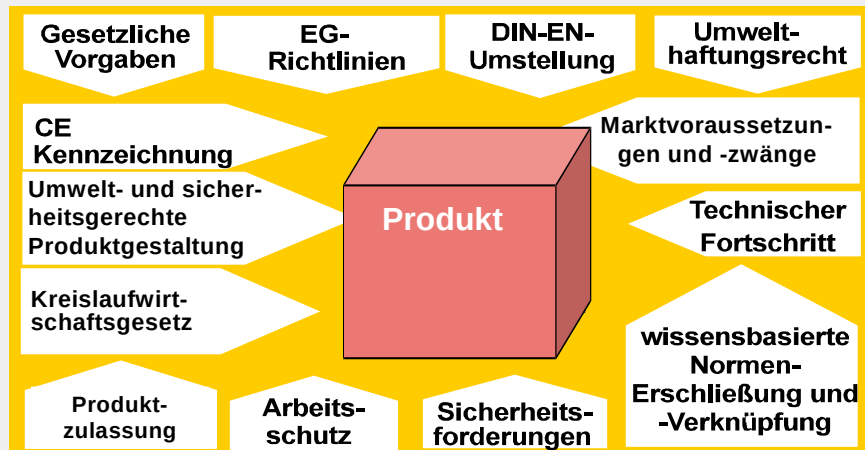
Rechtsver-
zeichnisse



3.4 Unternehmensspezifisches Betroffenheits- / Sicherheitsprofil (Risk-Manual)

Seite 21

Einflüsse auf das Produkt

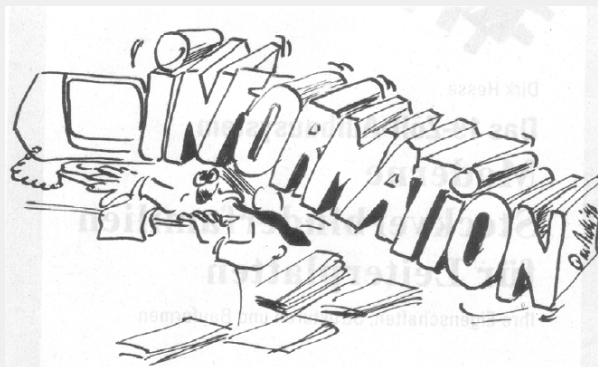


AGU – 2015
Wenglorz – ©

3.5 Informationsmenge

Seite 22

Viel zum Lesen



AGU – 2015
Wenglorz – ©

4. Ausgangsbasis: der moderne Risikobegriff



Andere Wurzel: „risc“ = arabisch für „Schicksal“

„Risiko“ etabliert sich im 14. Jahrhundert in den norditalienischen Stadtstaaten im Bereich des Seeversicherungswesens.

>>> Hintergrund: die hohe Verlustrate von Schiffen in dieser Zeit

➤ Definition **Risiko** in DIN EN ISO 9001:2015:

Auswirkung von Ungewissheit auf ein erwartetes Ergebnis

4. Ausgangsbasis: der moderne Risikobegriff

Nach ISO 31000 / ONR 49000ff:

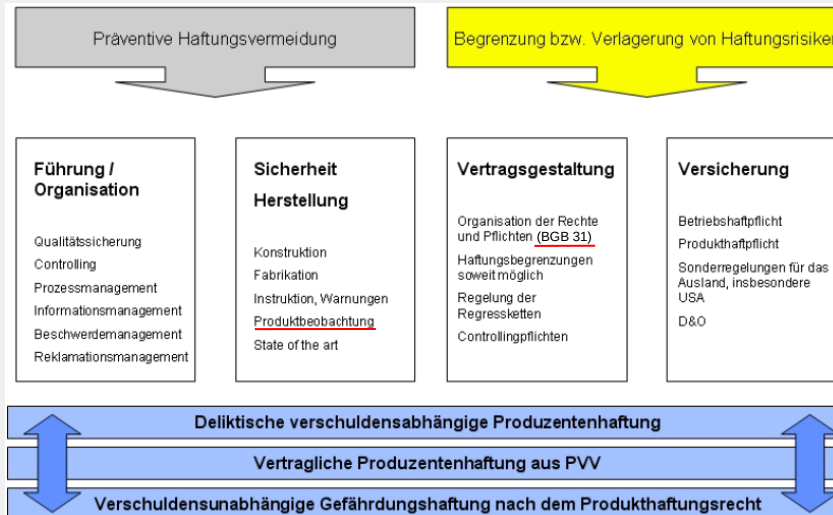
Auswirkung von Unsicherheit auf Ziele. Eine Auswirkung stellt eine Abweichung von Erwartungen dar - in positiver und/oder negativer Hinsicht.

Der Begriff Risiko umfasst folgende Gesichtspunkte:

- die Auswirkungen können positiv oder negativ sein,
- die Unsicherheit bzw. Ungewissheit wird mit Wahrscheinlichkeiten geschätzt bzw. ermittelt,
- die Ziele der Organisation oder des Systems umfassen strategische, operationelle oder finanzielle Ziele, die Sicherheit von Menschen, Sachen und der Umwelt („safety, security“) genauso wie andere Ziele und
- Risiko ist eine Folge von Ereignissen oder von Entwicklungen

Neue ISO 9001:2015 => Risikoorientiertes Auditieren (15 x Risiko...)

4. Ausgangsbasis: der moderne Risikobegriff Produzenten-Risikomanagement



5. Compliancemanagement

Definition:

Compliancemanagement umfasst alle notwendigen Tätigkeiten, um die Einhaltung nationaler und internationaler Gesetze, Vorschriften, Normen und Kodizes zu gewährleisten, samt zugehörigen Terminen und Meldegrenzen.

Anm.: Angesichts der Bedeutung von Compliance und der möglichen Folgen von Verstößen gegen Compliance-Anforderungen handelt es sich beim Compliance Management System um ein eigenständiges Management-System. Das Compliance Management System weist Berührungspunkte zu anderen Management-Systemen und Regelwerken auf (z.B. Corporate Governance, Risikomanagement, Qualitätsmanagement, Umweltmanagement, Betriebliches Kontinuitätsmanagement, Nachhaltigkeitsmanagement).

5.1 Begriffsklärung: Konformität vs. Compliance

Definition: „compliance“(engl.) = Beachten, Befolgen, Einhalten
Im betriebswirtschaftlichen Sinne beschreibt „Compliance“ das Einhalten von Gesetzen, Richtlinien, Normen, aber auch freiwilligen Kodizes.

Nach ISO/IEC 17000, Teil 1

➤ Konformität (conformity)

- Erfüllung einer Anforderung
 - Festgelegte Anforderungen können in normativen Dokumenten wie Rechtsvorschriften, Normen und technischen Spezifikationen niedergelegt sein.



➤ Compliance

- Handlung, Aktion: eine Organisation „complies (hält ein)“, in dem sie etwas **konform** macht oder
- **gesetzliche** Anforderungen erfüllt



5.2 Wofür Compliance Management ?

- unabdingbarer Rechtlicher Schutz

Das ständig wachsende und komplexer werdende Gefüge unterschiedlichster Vorgaben, z.B. in Bezug auf die

Zwänge durch Norm- /Rechtsforderungen machen ein strukturiertes, organisiertes Vorgehen zur Bewertung und Umsetzung aller Vorgaben für jedes Unternehmen **unerlässlich**, besonders im Hinblick auf die rechtliche Absicherung (Nachweispflicht) und strategische Unternehmensplanung.

5.3 Warum ist Compliance Management unerlässlich?

Seite 29

- unabdingbarer Rechtlicher Schutz

5.3.1. durch Normenforderung

„Die Organisation **muss** einen Prozess haben, um die rechtzeitige Bewertung, Verteilung und Verwirklichung aller technischen Normen, Vorgaben und Änderungen des Kunden [...] sicherzustellen“ (ISO/TS 16949:2009, Kap.4.2.3.1).

„Die Organisation **muss** Folgendes festlegen:
[...]

c) **gesetzliche und behördliche** Anforderungen, die auf das Produkt zutreffen, und

d) alle weiteren von der Organisation als notwendig erachteten **Anforderungen**“ (ISO/TS 16949, Kap. 7.2.1)

[Anm.: d.h. Normen, Regeln, Richtlinien, Gesetze etc.]

5.3 Warum ist Compliance Management unerlässlich?

Seite 30

- unabdingbarer Rechtlicher Schutz

5.3.2. durch Gesetzesforderungen

- Außerdem weist die Produzentenhaftung durch die Beweislastumkehr (Exkulpationsnachweis) den Unternehmen ein erheblich höheres Haftungsrisiko zu als bisher:

Nur wer sogenannte Entlastungstatbestände anführen kann und die rechtlich vorgegebene Sorgfaltspflicht erfüllt, wird in Zukunft die Haftung für Schäden verhindern können, die durch Sicherheitsmängel seiner Produkte herbeigeführt werden (**s.a. §§823/824 und 831 BGB Produzentenhaftung**).

- Jedes Unternehmen ist verpflichtet, sich zu organisieren, auch in Bezug auf die Bewertung und Umsetzung externer Vorgaben (**§31 BGB Organisationshaftung**). Daher können organisatorische Maßnahmen die Sicherstellung von Compliance/ Regelüberwachung im Unternehmen stützen.

5.3 Warum ist Compliance Management unerlässlich?

- unabdingbarer Rechtlicher Schutz

- Wer es laufen lässt und darauf baut, schon irgendwie über die Runden zu kommen, wird früher oder später unter großem Aufwand und Zeitdruck Versäumtes nachholen müssen, oder im schlimmsten Falle vor Gericht zur Verantwortung gezogen.
- Bei Verursachung eines Todesfalls durch **Organisationsverschulden** drohen den Geschäftsführern als Verantwortliche Leitung des Unternehmens sogar langjährige Haftstrafen wegen grober Fahrlässigkeit (z.B. Erdal-Urteil, etc.).
- Nur durch ein gelebtes und dokumentiertes CM-System kann eine „**gerichts feste Organisation**“ realisiert werden, die auch vor Gericht entlastend wirken kann.

5.3 Warum ist Compliance Management unerlässlich?

- unabdingbarer Rechtlicher Schutz

5.3.3 Die „gerichts feste“ Organisation



5.4 Projekt „gerichts feste Organisation“

Seite 33

- Keine Rechtssicherheit durch Delegation

- Rechtssicherheit kann nicht einfach von oben herab verordnet werden. Die Geschäftsleitung muss hierfür die Voraussetzungen schaffen (§ 31 BGB).
- Rechtssicherheit setzt die aktive Einbeziehung der Mitarbeiter voraus. Sie sind die Adressaten der rechtlichen Pflichten. Erst wenn sie ihre rechtliche Verantwortung kennen, haben sie die Chance, diese wirksam umzusetzen. Zum eigenen Schutz müssen sie wissen, wann, wie und wo sie zu handeln haben.
- Die große Herausforderung der Compliance-Systeme ist weniger die juristische Interpretation von Gesetzen, Regeln Richtlinien und Normen, als den Mitarbeitern die Fülle der rechtlichen und normativen Pflichten „zugänglich“ zu machen.

Resümee: starten eines Projektes „gerichts feste Organisation“

AGU – 2015
Wenglorz – ©

5.4 Projekt „gerichts feste Organisation“

Seite 34

Ziel des Projektes „gerichts feste Organisation“ sollte sein:

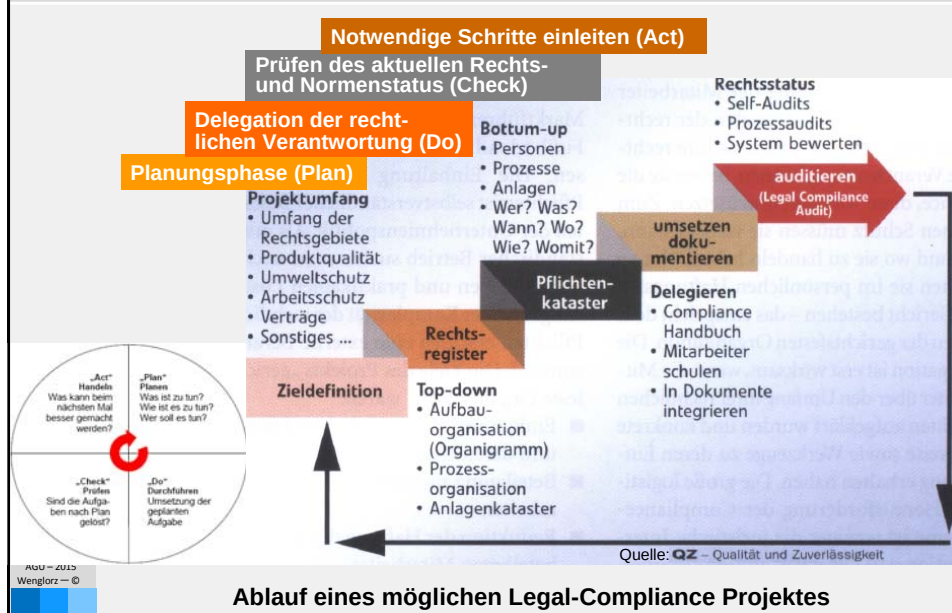
- Einhaltung aller rechtlichen und normativen Pflichten und deren Nachweis
- Beteiligung aller verantwortlichen Mitarbeiter
- Reduktion der Haftung der am System beteiligten Mitarbeiter
- Einfache Zugänglichkeit der rechtlichen und normativen Pflichten
- Verständliche und einfache umsetzbare Anweisungen an die Mitarbeiter
- Ordnungsgemäße und transparente Delegation
- Rückverfolgbarkeit der Pflichtenerfüllung
- Funktionale, prozess- und personenbezogene Zuordnung der rechtlichen Pflichten
- Nachweis der Rechtskonformität (Legal Compliance)
- Regelmäßige Aktualisierung der rechtlichen und normativen Pflichten durch ein Tool

AGU – 2015
Wenglorz – ©

5.4 Projekt „gerichts feste Organisation“

- Gerichtsfest nach bewährtem PDCA-Prinzip

Seite 35



5.5 Beispiel von Fragen der internen / externen Auditoren (1)

Seite 36

- ✓ Sind Ihnen die für Ihren Arbeitsbereich wesentlichen, gesetzlichen Forderungen zum Arbeits-, Sicherheits- und Umweltschutz bzw. zu den Produkteigenschaften bewusst – auch anwendungsorientiert bekannt?
- ✓ Woher (wissen) erfahren Sie, welche Gesetze, Normen, Richtlinien und weitere externe sowie interne Vorgaben für Ihren Bereich zu beachten sind und umgesetzt werden müssen?
- ✓ Wissen Sie, wo Sie diese jederzeit und schnell abrufen und einsehen?
- ✓ Bekommen Sie Informationen von extern (wie z.B. Abos, Internetseiten, sonstige Informationsquellen)?
- ✓ Welche Informationen erhalten Sie intern und von welchen internen Quellen?

5.5 Beispiel von Fragen der (internen) externen Auditoren (2)

Seite 37

- ✓ Wie läuft dieser Prozess ab?
- ✓ Werden alle Vorgaben gesammelt und dokumentiert?
- ✓ Wie setzen Sie (diese) Ihnen bekannte Vorgaben in Maßnahmen um?
- ✓ (Wie) wird die Einhaltung der Vorgaben überwacht? Wie oft geschieht das? Wird das dokumentiert?
- ✓ Ist dieser gesamte Ablauf von der Erfassung bis zur Umsetzung aller relevanten externen und internen Vorgaben **für Ihren Prozess/Bereich** als Prozess festgelegt und dokumentiert?

AGU – 2015
Wenglorz – ©

5.6 IGNORANZ: Compliancemanagement

Seite 38



IGNORANZ

Nichts sehen, hören, sagen:

Viele wollen die Compliance-Risiken nicht wahrnehmen.

AGU – 2015
Wenglorz – ©

5.7 Fazit: Compliance Management ist unerlässlich

- Die resultierenden Anwendungszwänge aus der stetig steigenden Anzahl an Gesetzen, Normen und sonstigen Vorgaben machen ein geplantes, zielgerichtetes Handeln unerlässlich.
- Ein gut organisiertes CM dient der rechtlichen Absicherung des Unternehmens, macht die externen Einflüsse auf die Unternehmen transparenter und somit die strategische Unternehmensplanung überschaubarer und leichter zu steuern.
- Des weiteren zeigt das CM einen Weg auf, alle Managementsysteme mit einem praktischen „Werkzeug“ ganzheitliches Vorgehen zu integrieren, und das ist...

2. Teil Das Dokumentenverwaltungsprogramm WISDOM

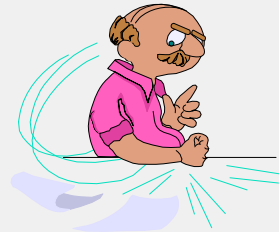
(Windows und Internet System für Dokumenten-Management)
um complianced zu werden und zu bleiben.





Fragen?

Diskussion!



Danke für Ihre
Aufmerksamkeit!

Hinweis:

In QZ-online.de ist ein Bericht über dieses Thema erschienen:

<https://www.qz-online.de/qualitaets-management/qm-basics/massnahmen/compliance-management/artikel/compliance-management-1080276.html>