



# Analyse von Normen/Regelwerken zur Ermittlung von Auditkriterien /-forderungen am Beispiel der **Unternehmenspolitik**.

Ausgabestand: 14.07.2011

Erstellt durch:

Peter Wintzer

Forderungen zur <b>Unternehmenspolitik</b> aus diversen Normen und Regelwerken	
Schritt 1:	Feststellung und Dokumentation der Forderungen zur <b>Unternehmenspolitik</b> verschiedener Normen und Regelwerke. Hier auszugsweise für das auf der PWMP-Webseite genannte Modellunternehmen der
Norm/Regelwerk	Textauszug zur Norm/zum Regelwerk
<b>ISO 9001:2008-12 und ISO/TS 16949:2009-11</b> <b>Abschnitt 5.3 = Qualitätspolitik</b> <i>Die oberste Leitung muss sicherstellen, dass die Qualitätspolitik</i> <i>a) für den Zweck der Organisation angemessen (1) ist,</i> <i>b) eine Verpflichtung zur Erfüllung von Anforderungen (2) und zur ständigen Verbesserung (3) der Wirksamkeit des Qualitätsmanagementsystems enthält,</i> <i>c) einen Rahmen zum Festlegen und Bewerten von Qualitätszielen (4) bietet,</i> <i>d) in der Organisation vermittelt (5) (6) und verstanden (7) wird und</i> <i>e) auf ihre fortdauernde Angemessenheit (8) bewertet wird.</i>	
<b>ISO 14001:2009-11 Abschnitt 4.2 und A.2 sowie EMAS III Anhang Teil A.2</b> <b>= Umweltpolitik</b> <i>Das oberste Führungsgremium muss die Umweltpolitik der Organisation festlegen (1) und sicherstellen, dass sie innerhalb des festgelegten Anwendungsbereiches (1) ihres UMS:</i> <i>a) in Bezug auf Art, Umfang und Umweltauswirkungen ihrer Tätigkeiten, Produkte und Dienstleistungen angemessen ist;</i> <i>b) eine Verpflichtung zur ständigen Verbesserung (3) und zur Vermeidung von Umweltbelastungen (9) enthält;</i> <i>c) eine Verpflichtung zur Einhaltung der geltenden rechtlichen Verpflichtungen und anderer Anforderungen (2) enthält, zu denen sich die Organisation bekennt, und die auf deren Umweltaspekte (9) bezogen sind;</i> <i>d) den Rahmen für die Festlegung und Bewertung der umweltbezogenen Zielsetzungen und Einzelziele (4) bildet;</i> <i>e) dokumentiert, implementiert und aufrechterhalten (8) wird;</i> <i>f) allen Personen mitgeteilt (5) (6) (7) wird, die für die Organisation oder in deren Auftrag (10) arbeiten; und</i> <i>g) für die Öffentlichkeit (11) zugänglich ist.</i> <b>EMAS III A.2:</b> <i>Falls die Organisation Teil einer übergeordneten Körperschaft ist, sollten die Festlegung und Dokumentation der Umweltpolitik (12) durch das oberste Führungsgremium der Organisation in Übereinstimmung mit der Umweltpolitik der übergeordneten Körperschaft und mit deren Freigabe (13) erfolgen.</i>	



# Analyse von Normen/Regelwerken zur Ermittlung von Auditkriterien /-forderungen am Beispiel der **Unternehmenspolitik**.

Ausgabestand: 14.07.2011

Erstellt durch:

Peter Wintzer

**ISO/IEC 27001:2008-09 Abschnitt 4.2.1 b) ISMS-Leitlinie; Abschnitt 5.1 Verpflichtung des Managements; Anhang A.5.1 Informationssicherheitsleitlinie 4.2.1 b):** Definition der ISMS-Leitlinie (1) unter Berücksichtigung der Eigenschaften des Geschäfts, der Organisation, ihres Standortes, ihrer Werte und ihrer Technologie, die:

- 1) einen Rahmen für Zielsetzungen (4) vorgibt und eine generelle Richtung sowie Grundsätze für Aktionen hinsichtlich Informationssicherheit festlegt;
  - 2) geschäftliche, gesetzliche und amtliche Anforderungen und vertragliche Sicherheitsverpflichtungen (2) berücksichtigt;
  - 3) mit dem strategischen Risikomanagementkontext (14) der Organisation abgestimmt (13) ist, in dem die Einrichtung und Instandhaltung des ISMS erfolgen wird;
- 5.1:** Das Management muss seine Verpflichtung für die Festlegung, Umsetzung, Durchführung, Überwachung, Überprüfung, Instandhaltung und Verbesserung (3) des ISMS nachweisen, indem es:
- a) eine ISMS-Leitlinie (1) festlegt;
  - b) sicherstellt, dass die Ziele (4) und Pläne für das ISMS festgelegt werden;
  - c) Aufgaben und Verantwortlichkeiten für Informationssicherheit bestimmt;
  - d) der Organisation die Bedeutung des Erreichens von Informationssicherheitszielen und der Einhaltung der Informationssicherheitsleitlinien vermittelt (7), genauso wie die Verantwortlichkeiten im Rahmen des Gesetzes und die Notwendigkeit für kontinuierliche Verbesserung (3);

## **Anhang A.5.1 Informationssicherheitsleitlinie**

Ziel: Richtungsvorgabe (1) und Unterstützung des Managements bei der Informationssicherheit, in Übereinstimmung mit Geschäftsanforderungen und geltenden Gesetzen und Regelungen (2).

**A.5.1.1 Leitlinie zur Informationssicherheit:** Das Management muss eine Informationssicherheitsleitlinie (1) genehmigen, veröffentlichen (11) und alle Angestellten (5) und relevanten Externe (10) davon in Kenntnis setzen.

**A.5.1.2 Überprüfung der Informationssicherheitsleitlinie:** Die Informationssicherheitsleitlinie muss in regelmäßigen Abständen (8) und immer dann überprüft werden, wenn wesentliche Änderungen (6) erfolgen, um ihre Eignung, Angemessenheit und Wirksamkeit auf Dauer sicherzustellen.

## **ISO 31000:2010 4.2 Mandat und Verpflichtung; 4.3.2 Festlegung der Risikomanagementpolitik**

**4.2:** Die Einführung des Risikomanagements und die Gewährleistung seiner anhaltenden Wirksamkeit erfordern eine starke und dauerhafte Verpflichtung durch die oberste Leitung der Organisation sowie eine sorgfältige, strategische Planung, um auf allen Ebenen ein Engagement zu erreichen. Die oberste Leitung sollte:

- **eine Risikomanagementpolitik** (1) festlegen und mittragen,
- **sicherstellen**, dass die Kultur der Organisation (1) und die Risikomanagementpolitik miteinander im Einklang stehen,
- **Leistungsindikatoren** (14) für das Risikomanagement festlegen, die mit den Leistungsindikatoren der Organisation vereinbar sind,
- **die Ziele** des Risikomanagements auf die Ziele (4) und Strategien der Organisation abstimmen,
- **die Einhaltung** rechtlicher und regulatorischer Bestimmungen (2) gewährleisten,
- **Verantwortlichkeiten** und Zuständigkeiten auf entsprechenden Ebenen in der Organisation festlegen;
- **sicherstellen**, dass die erforderlichen Ressourcen dem Risikomanagement zugeteilt werden,
- **die Vorteile** (15) des Risikomanagements allen Stakeholdern (5) (10) vermitteln,
- **gewährleisten**, dass der Rahmen für das Behandeln von Risiken seine Angemessenheit (8) weiterhin behält.



## Analyse von Normen/Regelwerken zur Ermittlung von Auditkriterien /-forderungen am Beispiel der **Unternehmenspolitik.**

Ausgabestand: 14.07.2011

Erstellt durch:

Peter Wintzer

**4.3.2:** Die Risikomanagementpolitik sollte die Ziele (4) und das Engagement der Organisation für das Risikomanagement klar darlegen und in der Regel folgende Aspekte behandeln:

- **die Begründung** (15) der Organisation für die Behandlung von Risiken,
- **Verknüpfungen** zwischen den Zielen (4) C10 und Politiken der Organisation und der Risikomanagementpolitik,
- **Verantwortlichkeiten** und Zuständigkeiten für die Behandlung von Risiken
- **Vorgehensweise** bei Interessenkonflikten
- **Verpflichtung** zur Bereitstellung der erforderlichen Ressourcen zur Unterstützung der für die Behandlung von Risiken zuständigen und verantwortlichen Personen,
- **Modalitäten** der Messung der Leistung des Risikomanagements und der Berichterstattung darüber,
- **Verpflichtung** zur Überprüfung und Verbesserung (3) der Risikomanagementpolitik und des Rahmens in regelmäßigen Intervallen (8) sowie aufgrund von Ereignissen und Entwicklungen.

Die Risikomanagementpolitik sollte entsprechend kommuniziert (7) (6) (10) werden.

### **OHSAS 18001:2007-11 4.2 A&G-Politik**

Das oberste Führungsgremium muss die A&G-Politik der Organisation festlegen (1) und sicherstellen, dass sie innerhalb des festgelegten Anwendungsbereiches (1) ihres A&G-Managementsystems.

- a) in Bezug auf Art und Umfang der A&G-Risiken der Organisation angemessen (1) ist,
- b) eine Verpflichtung zur Vermeidung von Verletzungen und Erkrankungen (2) sowie zur ständigen Verbesserung (3) des A&G-Managementsystems und der A&G-Leistungen;
- c) eine Verpflichtung zur Einhaltung der geltenden rechtlichen Verpflichtungen und anderen Anforderungen (2) enthält, zu denen sich die Organisation bekennt und die sich auf ihre A&G-Risiken beziehen;
- d) den Rahmen für die Festlegung und Bewertung der A&G-Zielsetzungen (4) bildet;
- e) dokumentiert (1), implementiert (7) und aufrechterhalten (8) wird;
- f) allen Personen mitgeteilt wird, die für die Organisation (5) oder in deren Auftrag (10) arbeiten, damit diese sich ihrer jeweiligen A&G-Verpflichtungen bewusst werden;
- g) für die Öffentlichkeit zugänglich (11) ist und
- h) regelmäßig überprüft (8) wird, um sicherzustellen, dass sie für die Organisation relevant und angemessen (6) bleibt.



## Analyse von Normen/Regelwerken zur Ermittlung von Auditkriterien /-forderungen am Beispiel der **Unternehmenspolitik.**

Ausgabestand: 14.07.2011

Erstellt durch:

Peter Wintzer

### **VDA Band 6 Teil 1 Abschnitt 01 Verantwortung der Leitung**

01.1\* Ist die Qualitätspolitik von der Leitung des Unternehmens festgelegt und auf allen Ebenen bekannt gemacht worden? (1) (2) (4) (5) (7) (16)

01.2\* Sind im Rahmen der Unternehmensplanung bzw. der Qualitätspolitik Qualitätsziele festgelegt, werden die Ergebnisse überwacht? (4)

01.3\* Ist ein kontinuierlicher Verbesserungsprozess Bestandteil der Qualitätspolitik? (3)

01.6\* Bewertet die Leitung regelmäßig die Wirksamkeit des QM-Systems? (6) (8)

(\* = besonderer Einfluss auf Produkt und Prozess)

Schritt 2:

Analyse der in Schritt 1 ausgewiesenen Forderungen auf Übereinstimmung und auf Zusatzforderungen.  
Das Analyseergebnis ist als Auditkriterium / -forderung im 3. Schritt in der gleichnamigen Spalte ausgewiesen.



## Analyse von Normen/Regelwerken zur Ermittlung von Auditkriterien /-forderungen am Beispiel der **Unternehmenspolitik.**

Ausgabestand: 14.07.2011

Erstellt durch:

Peter Wintzer

Schritt 3: Zuordnung der einzelnen Normen- bzw. Regelwerkabschnitte zu den Auditkriterien / -forderungen. Sind in einer Zeile mehrere Abschnitte aufgeführt, ist dieses darauf zurückzuführen, dass die Forderung mehrfach aufgeführt ist.									
Nr.:	Auditkriterium / -forderung	ISO 9001: 2008-12	ISO/TS 16949: 2009-11	ISO 14001: 2009-11	EMAS III	ISO/IEC 27001: 2008-09	ISO 31000: 2009	OHSAS 18001: 2007-11	VDA 6.1:2003
1	Ist eine für die Organisation relevante und angemessene Politik und ihr Anwendungsbereich festgelegt und dokumentiert?	4.2.1 5.1 5.3	4.2.1 5.1 5.3	4.2 4.4.4	A-AII-A.2 A-AII-A.4.4	4.2.1 b) 5.1 Anh. 5.1 A.5.1.1	4.2	4.2 4.4.4	01.1*
2	Enthält die Politik eine Verpflichtung an alle Mitarbeiterinnen und Mitarbeiter zur Erfüllung von Anforderungen (externe und interne)?	5.1 5.3	5.1 5.3	4.2 4.3.3	A-AII-A.2 A-AII-A.3.3 B-AII-B.2	4.2.1 b) 5.1	4.2	4.2 4.3.3	01.1*
3	Sind Aussagen zum Prozess der kontinuierlichen Verbesserung Bestandteil der Politik?	5.3	5.3	4.2	A-AII-A.2 B-AII-B.3 B-AII-B.4.1	5.1	4.3.2	4.2 4,3,3	01.3*
4	Ist die Politik geeignet, aus ihr Ziele ableiten zu können?	5.3 5.4.1	5.3 5.4.1	4.2	A-AII-A.2	4.2.1. b)	4.2 4.3.2	4.2 4.3.3	01.1* 01.2*
5	Wurden Politik und Leitsätze in geeigneter Weise dem Personal bekannt gemacht?	5.3	5.3	4.2 4.4.2	A-AII-A.2 A-AII-A.4.2	A.5.1.1	4.2 4.3.2	4.2 4.4.2	01.1*
6	Sind Veröffentlichungen zu Unternehmenspolitik und -zielen aktuell?	5.3 5.4.1	5.3 5.4.1	4.2 4.3.3	A-AII-A.2 A-AII-A.3.3	A.5.1.2	4.3.2	4.2 4.3.3	01.6*
7	Sind Politik und Leitsätze allen Beschäftigten bekannt?	5.3	5.3	4.2	A-AII-A.2	5.1 A.5	4.3.2	4.2	01.1*
8	Ist die Politik mindestens einmal im Jahr auf Angemessenheit geprüft und sind ggf. erforderliche Änderungen vorgenommen worden?	5.3	5.3	4.2 4.6	A-AII-A.2 A-AII-A.6	A.5.1.2	4.2 4.3.2 4.5	4.2 4.6	01.6*
9	Beinhaltet die Politik auch Aussagen zur Feststellung und Vermeidung von Gefährdungen, die durch die Geschäftstätigkeit der Organisation entstehen können?			4.2	A-AII-A.2		4.3.2	4.2 4.3.3	
10	Ist gewährleistet, dass die Politik auch allen externen Lieferanten / Dienstleistern bekannt ist, einschl. denen, die auf dem Gelände der Organisation tätig sind?			4.2	A-AII-A.2	A.5.1.1	4.2 4.3.2	4.2	
11	Ist die Politik auch der Öffentlichkeit zugänglich?			4.2	A-AII-A.2	A.5.1.1		4.2	
12	Wurde in den erforderlichen Fällen für den jeweiligen Standort eine eigene Politik festgelegt und dokumentiert?			4.2	A-AII-A.2 B-AII-B.3				
13	Wurde in den zutreffenden Fällen die jeweilige Politik mit der Politik der Konzernzentrale abgestimmt?			4.2	A-AII-A.2	4.2.1. b)			



## Analyse von Normen/Regelwerken zur Ermittlung von Auditkriterien /-forderungen am Beispiel der **Unternehmenspolitik.**

Ausgabestand: 14.07.2011

Erstellt durch:

Peter Wintzer

14	Liegt ein strategisches Konzept zur Feststellung und Behandlung von Risikosituationen vor, die in Geschäftsprozessen oder an Produkten auftreten können?					4.2.1. b) A.14	4.2		
15	Wurde allen am Risikomanagementprozess Beteiligten (intern/extern) dessen Nutzen vermittelt?						4.2 4.3.2		
16	Ist die Null-Fehlerstrategie Bestandteil der Politik?								1.1*

Schritt 4:	Auditkriterien / -forderungen den Tätigkeitsschritten zuordnen, und Details zur Auditdurchführung festlegen (hier Bestandteil des Auditmanagers von WissIntra).			
Nr.:	Auditkriterium / -forderung	Tätigkeitsschritt	Erläuterung	Prüfmöglichkeit
1	Ist eine für die Organisation relevante und angemessene Politik und ihr Anwendungsbereich festgelegt und dokumentiert?	A121 Politik /Strategie / Leitsätze) festlegen	Dieses schließt die Übereinstimmung mit der Organisationskultur sowie Begriffe wie Mission oder Vision ein, beinhaltet immer die Qualitätspolitik und je nach Normenforderung auch zusätzliche Kriterien wie z. B. Umwelt, Sicherheit, Risiko, IT	Sichtung Managementhandbuch, Aushänge, Internetveröffentlichungen
2	Enthält die Politik eine Verpflichtung an alle Mitarbeiterinnen und Mitarbeiter zur Erfüllung von Anforderungen (externe und interne)?	A121 Politik /Strategie / Leitsätze) festlegen	Dieses schließt die Selbstverpflichtung der obersten Leitung ein.	Sichtung Managementhandbuch, Aushänge, Internetveröffentlichungen
3	Sind Aussagen zum Prozess der kontinuierlichen Verbesserung Bestandteil der Politik?	A121 Politik /Strategie / Leitsätze) festlegen		Sichtung Managementhandbuch, Aushänge, Internetveröffentlichungen
4	Ist die Politik geeignet, aus ihr Ziele ableiten zu können?	A121 Politik /Strategie / Leitsätze) festlegen	Abgleich der Texte der Politik mit den konkreten Zielsetzungen der Organisation.	Sichtung Managementhandbuch, Aushänge, Internetveröffentlichungen
5	Wurden Politik und Leitsätze in geeigneter Weise den Mitarbeitern bekannt gemacht?	A121 Politik /Strategie / Leitsätze) bekannt machen	- beinhaltet ggf. auch Mission und Vision - Politik, z. B. in Form von Leitsätzen, Leitlinien	Frage nach Aushang, Werkszeitung, Info-Veranstaltung u. ä.
6	Sind Veröffentlichungen zu Unternehmenspolitik und -zielen aktuell?	A121 Politik /Strategie / Leitsätze) festlegen	Hierzu zählen u. a. Aushänge an Info-Tafeln oder Beschreibungen im Internet.	Abgleich der veröffentlichten Unterlagen mit den Daten der Quelldokumente
7	Sind Politik und Leitsätze allen Beschäftigten bekannt?	A121 Politik /Strategie / Leitsätze) bekanntmachen		Stichprobenhafte Befragung von Beschäftigten
8	Ist die Politik mindestens einmal im Jahr auf Angemessenheit geprüft und sind ggf. erforderliche Änderungen vorgenommen worden?	A121 Politik /Strategie / Leitsätze) festlegen		Prüfen, ob die Politik im Rahmen der Managementsystembewertung auch betrachtet wurde.
9	Beinhaltet die Politik auch Aussagen zur Feststellung und Vermeidung von Gefährdungen, die durch die Geschäftstätigkeit der Organisation entstehen können?	A121 Politik /Strategie / Leitsätze) festlegen	betrifft u.a. auch Umwelt-, Arbeits- und Gesundheitsschutz	Sichtung Managementhandbuch, Aushänge, Internetveröffentlichungen



## Analyse von Normen/Regelwerken zur Ermittlung von Auditkriterien /-forderungen am Beispiel der **Unternehmenspolitik.**

Ausgabestand: 14.07.2011

Erstellt durch:

Peter Wintzer

10	Ist gewährleistet, dass die Politik auch allen externen Lieferanten / Dienstleistern bekannt ist, einschl. denen, die auf dem Gelände der Organisation tätig sind?	A121 Politik /Strategie / Leitsätze)bekannt machen		Während des Audits Mitarbeiter/innen von Fremdfirmen befragen.
11	Ist die Politik auch der Öffentlichkeit zugänglich?	A121 Politik /Strategie / Leitsätze)bekannt machen		Frage nach Art der Veröffentlichung stellen wie. Z. B. im Internet.
12	Wurde in den erforderlichen Fällen für den jeweiligen Standort eine eigene Politik festgelegt und dokumentiert?	A121 Politik /Strategie / Leitsätze) festlegen	Trifft nur für Organisationen zu, die Konzernzugehörig sind und nicht eigenständig über ihre Politik entscheiden können.	Sachverhalt bei der Unternehmensleitung abfragen
13	Wurde in den zutreffenden Fällen die jeweilige Politik mit der Politik der Konzernzentrale abgestimmt?	A121 Politik /Strategie / Leitsätze) festlegen	Trifft nur für Organisationen zu, die Konzernzugehörig sind und nicht eigenständig über ihre Politik entscheiden können.	Sachverhalt bei der Unternehmensleitung abfragen
14	Liegt ein strategisches Konzept zur Feststellung und Behandlung von Risikosituationen vor, die in Geschäftsprozessen oder an Produkten auftreten können?	A121 Politik /Strategie / Leitsätze) festlegen	Richtlinie der obersten Leitung zur Erfassung von und zum Umgang mit Risikosituationen, die auch Bewertungskriterien und Genehmigungsverfahren beinhaltet.	Sachverhalt bei der Unternehmensleitung abfragen
15	Wurde allen am Risikomanagementprozess Beteiligten (intern/extern) dessen Nutzen vermittelt?	A121 Politik /Strategie / Leitsätze)bekannt machen		Stichprobenhafte Befragung von Beschäftigten
16	Ist die Null-Fehlerstrategie Bestandteil der Politik?	A121 Politik /Strategie / Leitsätze) festlegen	Die Umsetzung betrifft nicht nur das Innenverhältnis, sondern muss ggf. auch auf Lieferanten übertragen werden.	Sichtung Managementhandbuch, Aushänge, Internetveröffentlichungen