Leitfaden

Leitlinie Integriertes Managementsystem (IMS)

16.11.2018

Inhalt

Hinweis: In dieser Dokumentation gibt es einige Links, die es den AEB-Mitarbeitern ermöglichen, weitere Informationen im AEB-Intranet zu öffnen. Dies verdeutlicht den hohen Integrationsgrad des Wissensmanagements der AEB.

1 Leitlinie und Regeln zur Politik der Qualität und der Informationssicherheit

Dieses Dokument ist eine umfassende Leitlinie der AEB zur Beschreibung ihrer Qualitätsansprüche. Die darin integrierte Informationssicherheitsleitlinie richtet sich an die von der Informationssicherheit Betroffenen und regelt das Management der Sicherheit.

Inhaltlich orientiert sich diese Leitlinie dazu nach der neuen **High-Level-Struktur** der novellierten ISO-Normen **ISO 9001** und **ISO 27001** in den Fassungen seit ca. 2014.

Dabei werden in dieser Leitlinie folgende Kapitel bedient:

Kapitel der ISO-Norm	Inhalte, Zwecke	Hier zu finden in
4 – Umfeld der Organisation	• Verständnis der Organisation • Interessierte Parteien und ihre Erwartungen • Anwendungsbereiche zu Qualitätsmanagementsystem bzw. Informationssicherheitsmanagementsystem	Abschnitt 1.2 Abschnitt 1.2 Abschnitt 1.3
5 – Führung(sverhalten)	• Führung und Selbstverpflichtung • Qualitätspolitik • Aufgaben, Verantwortung, Befugnis	Abs.1.1, Abs. 4.1.1 Abschnitt 2.1 Abschnitt 4.1.3
6 – Planung	• (Umgang mit) Risiken und Chancen • Qualitätsziele • Planung von Veränderungen	Abschnitt 4.2 Abschnitt 2.1 Abschnitt 4.3
7 - Unterstützung	• Ressourcen • Kompetenz • Bewusstsein • Kommunikation • Dokumentierte Informationen	Abs. 3.1, Abs. 3.2 Abschnitt 3.3 Abschnitt 3.3 Abschnitt 3.4 Abschnitt 3.5

Die obigen Norm-Kapitel 4-7 umfassen die **Plan-Phase aus dem prozessorientierten Zyklus PDCA**.

Strukturell haben wir in dieser Leitlinie der AEB eine eigene Kapitel-Einteilung gewählt:

- **Kapitel 1** widmet sich den großen Zielen und Anforderungen, dem Selbstverständnis der AEB mit Blick auf Qualität und Sicherheit
- **Kapitel 2** schließt mit Aussagen zu den Anwendungsbereichen der Managementsysteme
- **Kapitel 3** widmet sich der Organisation, in der Mensch im Mittelpunkt steht und in seinen Rollen mit Verantwortung Aufgaben wahrnimmt
- **Kapitel 4** widmet sich dem Prozessorientierten Ansatz PDCA. und macht dabei auch Aussagen zu den verbleibenden Kapiteln 8-10 der ISO-Norm.

Dabei gilt folgende Kapitel-Zuordnung für die Phasen DCA:

Kapitel der ISO-Norm	Funktion, Inhalt	PDCA-Phase	Hier zu finden in
8 - Operativer Betrieb	Operativer Betrieb / Einsatz	Do	Abschnitt 4.5
9 - Leistungsbewertung	Leistungsbewertung (Sicherstellung von Kontrolle und Wirksamkeit)	Check	Abschnitt 4.6
10 - Verbesserung	Verbesserung	Act	Abschnitt 4.7

Wir versuchen hier die Aussagen für die Managementsysteme für Qualität und Sicherheit zusammen darzustellen, spezielle Aussagen zu Qualität oder Sicherheit finden sich zur Verbesserung der Lesbarkeit in separaten Abschnitten.

1.1 Zweck und grundsätzlicher Anspruch

Diese Leitlinie will sich einigermaßen stabil erhalten; sie ist auch Bestandteil der Unternehmenskultur und ist **Ausdruck und Willenserklärung des Top-Managements**. Sie umfasst Politikerklärungen als Obermenge zur Qualität und Informationssicherheit (Rahmen zum Setzen von Zielen, Handlungsgrundsätze u.ä.). Eine wesentliche Orientierung bieten die **ISO 9001** und die **ISO 27001**, zu der wir seit Februar 2010 im Besitz eines Zertifikats sind.

- Regeln ändern sich; wir leben in einer dynamischen Welt.
- Qualität und Security bedeuten zuerst Bewusstsein.
- Qualität und Security ist ein Anspruch, dessen Verwirklichung trainiert werden muss. Daher verstehen wir Qualitätsmanagement als eine Verpflichtung, eine grundsätzliche Einstellung und einen Prozess der kontinuierlichen Verbesserung. Wir sind auf langfristige Beziehungen ausgerichtet. Security sehen wir als einen Bestandteil, einen Blickwinkel der Qualität.

1.2 Vorgaben und Anforderungen

Ziel: Welche Vorgaben welcher interessierter Parteien beschreiben den Kontext der Organisation und beeinflussen somit die Konformität?

Als Übersicht:

Partei	Interessen	Schnittstellen	Wie im Griff?
Kunden	Erfüllung der vertraglich zugesicherten Leistungen; Produkt-Erwartungen gemäß aktuellen Markt-Erfordernissen nach Stand der Technik; u.a. auch der Rechtskonformität	Allgemeine Geschäftsbedingungen (AGB); Vertragliche Bindung (Lizenz, Support, SLA, NDA, ...); Aussagen in Leistungsbeschreibungen	Produktmanagement, Recht, Services-Organisation (u.a. SLA-Management)
Gesetzgeber	Compliance	Vermittlung u.a. über Weiterbildung	Team Recht; Datenschutzbeauftragter;

			Zentrales Vertragsmanagement; Compliance Officer
Dienstleister	Vergütung	(Service-) Verträge	Partnermanager; übergreifendes Partnermanagement mit Kontroll-Funktionen
Partner	Vergütung; partnerschaftliche Begleitung für die gemeinsamen Ziele samt Ausrichtung	(Partner-) Verträge	Partnermanager; Kontrollen; regelmäßiger Austausch
Endverbraucher	Usability, Performance der Anwendungen; verfügbare Hotline	Leistungsbeschreibungen, Online-Hilfen, Support	Produktmanagement, Marketing, Rückmeldungen u.a. aus Seminaren; Support-Organisation
Zollbehörde	Kommunikation nach zertifizierten Verfahren	Zertifizierte Verfahren	Produktmanagement

Weitere Ausführungen:

Geschäftserfordernisse

Unsere Kunden stehen im Fokus unseres Qualitätsanspruchs; deren Vertrauen und Zufriedenheit mit den Lösungen der AEB hinsichtlich Unterstützung deren Geschäftsprozesse ist elementares Maß für den Erfolg. Dabei sind wir aufgrund unserer Hosting-Lösungen auch angehalten, die Sicherheits- und Qualitäts-Ansprüche zu erfüllen, die sich z.B. aus gesetzlichen Anforderungen für unsere Kunden und deren Prozesse ergeben. Die Einhaltung von Sicherheitsmaßstäben ist daher für die AEB in hohem Maße durch ihre Rolle und Aktivitäten als Dienstleister in ihrem Branchenumfeld gegeben. Die Internationalisierung legt daher die Orientierung an international anerkannten Maßstäben nahe. Der Qualitätsanspruch leitet sich bereits unmittelbar aus den Rahmenbedingungen und Anforderungen im Einsatz der Produkte ab. Die AEB nimmt die Perspektive Sicherheit als zunehmend wichtiges Entscheidungskriterium im Markt wahr. Die Perspektive Sicherheit beschränkt sich dabei nicht allein auf die Beherrschung der Facette Technik, sondern berücksichtigt organisatorische Aufstellung und die Beachtung gesetzlicher Anforderungen gerade auch in unserem Umfeld unserer Produkte und Dienstleistungen, mit denen unsere Kunden täglich Geschäftsprozesse durchführen.

Gesetzliche Anforderungen

Mit Kurzbeschreibung in Stichworten:

- KonTraG (Maßgabe, ein Überwachungssystem einzurichten; Früherkennung; Aussagen über Risikostruktur; Nachweis der Nachvollziehbarkeit über die Funktion eines Kontrollsystems)

- GDPdU, GOBS (Sorgfaltspflichten bei der Verarbeitung, Vorhaltung und Bereitstellung von Informationen, insbesondere zu rechnungsrelevanten Daten zur Buchführung und Steuerprüfung; Forderung zur Einrichtung eines internen Kontrollsystems)
- DSGVO, BDSG (Bereitstellung eines Sicherheitskonzepts nach Art. 32 DSGVO – techn. und organisatorische Maßnahmen; Sorgfalt hinsichtlich Persönlichkeitsrechten Betroffener, Datensparsamkeit, Vertraulichkeit, Zweckgebundenheit, usw.)
- Basel III (indirekt über Vorgaben an Banken als Kreditgeber)
- Relevante Gesetze und (Branchen-)Vorgaben im Außenhandel Die Applikationen der AEB bewegen sich in einem sensiblen, sehr dynamischen und internationalen Umfeld, in dem länderspezifische oder -übergreifende Politik Einfluss darauf nimmt, was gerade als korrekt und compliant gilt. Einige Stichworte hierzu: Ausfuhrbeschränkungen, Kriegswaffen nach KKWG, Rüstungsgüter nach AWV, Dual-Use, Embargolisten. Somit sind auch Ämter wie das BAFA (Bundesamt für Wirtschaft und Ausfuhrkontrolle) wichtige Quellen.

Vertragliche Anforderungen

- Im Rahmen von Service Level Agreements (SLA) mit Kunden vereinbaren wir Qualitätsziele und deren Einhaltung mit quantitativen Angaben (u.a. Reaktionszeiten, Verfügbarkeiten).
- Die DSGVO gibt uns Vorschriften vor, die uns im Umgang mit unseren Kunden, Partnern und Subunternehmern zu besonderen Sorgfaltsplichten anleiten (s. Auftragsverarbeitung nach Art. 28 DSGVO). Ein Datenschutzbeauftragter ist benannt.
- Abschluss von Vertraulichkeitserklärungen mit Geschäftspartnern (Kunden, Partner, Subunternehmer); im Innenverhältnis werden die Mitarbeiter zur Geheimhaltung verpflichtet und für den vertraulichen Umgang mit Informationen sensibilisiert und regelmäßig geschult.
- Mit Subunternehmern werden Vertraulichkeitserklärungen abgeschlossen. In Fällen mit Systemzugang (etwa zu Zwecken von Wartung eingesetzter Applikationen) werden gesonderte Systemzugangsverträge abgeschlossen und die Zugänge und Zugriffe dabei auf das erforderliche Maß beschränkt.

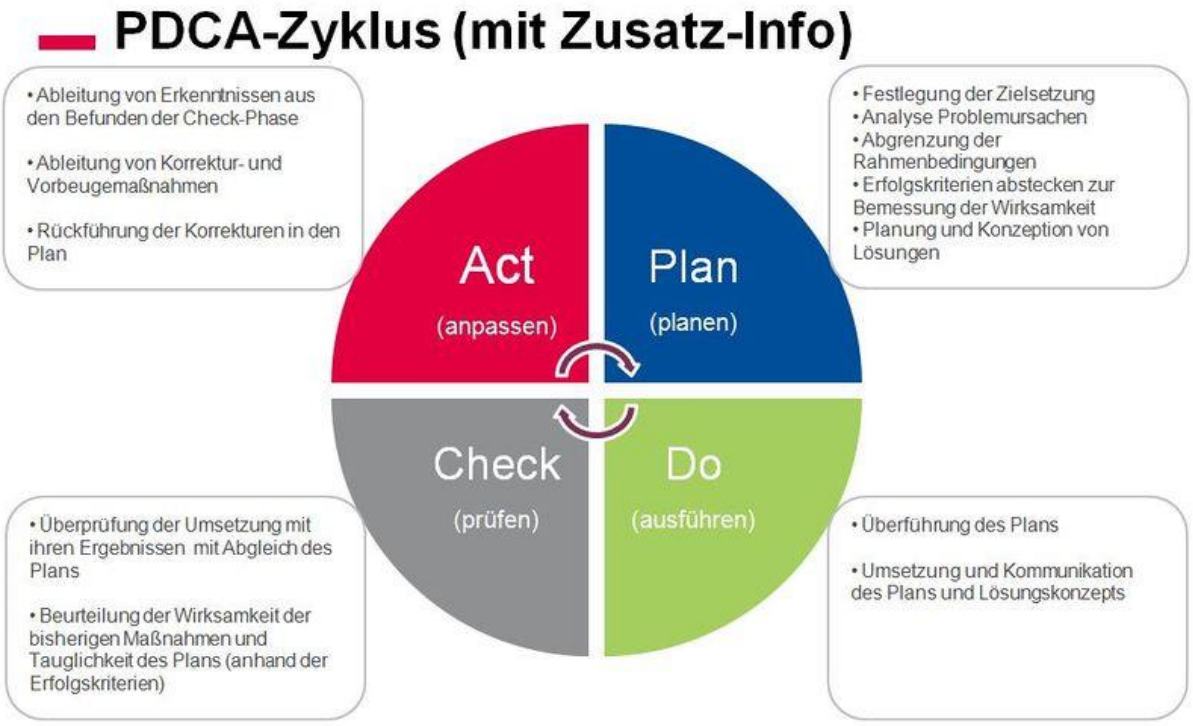
Sonstige regulative Anforderungen

Alle Mitarbeiter der Organisation sind zur Einhaltung obiger Erfordernisse und Anforderungen aufgerufen und verpflichtet. Generell ist jeder Mitarbeiter verantwortlich, zur Qualitätssicherung aktiv beizutragen. Das Bewusstsein, die Wachsamkeit und die tatsächliche Wahrnehmung von qualitätssichernden Maßnahmen sowie das Training z.B. auch von Notfall-Management werden

- im Rahmen von Pflicht-Schulungen der AEB geschult,
- in Meetings der Securityverantwortlichen bzw. der Qualitätsmanager kontinuierlich überwacht
- und regelmäßig im Rahmen von internen Audits geprüft

Zur Erfüllung der Nachhaltigkeit (wirksame Sicherstellung des ISMS und QMS):

- ist ein PDCA-Zyklus aufgesetzt, aus dem auch Verantwortlichkeiten und Spielregeln hervorgehen



- sind alle Mitarbeiter aufgerufen, den jeweilig Verantwortlichen einzuschalten, wenn sich Änderungen im Umfeld ergeben, die Auswirkungen auf Sicherheit oder Qualität haben könnten.
- Orientierung an den Vorgaben der Normen ISO 9001 und ISO 27001 und den zugehörigen Managementsystemen

1.3 Anwendungsbereiche

Zur ISO 9001 – Verfahren und Prozesse

Der **Anwendungsbereich** bezieht sich auf das gesamte Unternehmen und umfasst somit:

- alle Standorte
- alle Produkte

Begründung für die Auswahl

Mit der zunehmenden Bedeutung von Software und Dienstleistungen in wertschöpfenden Prozessen von Unternehmen (AEB Kunden) steigt auch deren Anspruch an die Qualität der AEB Softwareprodukte. AEB ist es wichtig, die Kunden mit Lösungen und Services zu überzeugen, die auch langfristig die an sie gehegten Erwartungen erfüllen und dabei höchsten Qualitätsansprüchen genügen.

Zur ISO 27001 - Verfahren und Prozesse

Der Anwendungsbereich sind die AEB-Kunden-Rechenzentren in Stuttgart sowie die Softwareentwicklung.

- Örtlichkeit: Stuttgart, Sigmaringer Str. 109
- System: Betrieb der gehosteten Systeme sowie weitere Services für unsere Kunden; dies betrifft alle Anwendungen der AEB

- Schnittstellen: Dies sind Zugangssysteme für remote-Zugriffe (CITRIX-Server, WebServer für Internet-Anbindungen …), Verbindungen z.B. zum Zoll.
- Werte: Eine ausführliche Auflistung der Werte und Risiken erfolgt im hierfür vorgesehenen Werkzeug zum Risikomanagement. Angrenzende Prozesse sind dabei
  - Service/Support: Prozess Changemanagement
  - Kundenprojekte: Prozess Releasemanagement
  - Facility Management für die Kunden-Rechenzentren
  - Zuleistungen von Partnern: Prozess Partnermanagement; bei Zugängen mit Partnerverträgen für Systemzugang

Begründung für die Auswahl

- Konzentration auf die Kernfunktionalität
- Der Schutzbedarf zu Betrieb Rechenzentrum ist hoch
- Die Kunden-Rechenzentren und die Produktentwicklung nehmen einen bedeutenden Anteil unseres Business ein

2 Die Managementsysteme QMS und ISMS im IMS

Prozessorientierte Managementsysteme sorgen für Betrieb und laufende Verbesserung.

Dazu zählen u.a.

- eine Leitlinie mit der Klarstellung der Zielsetzung und Organisation
- Werkzeuge für Monitoring der Wirksamkeit
- Administrative Instrumente und prozessorientiertes Arbeiten für Betrieb, Überprüfung und Verbesserung
- Risikomanagement

Die Ziele der Managementsysteme sind regelmäßig zu kommunizieren und bei Bedarf zu aktualisieren.

2.1 Leitsätze zur Qualitätspolitik

AEB-Qualitätsanspruch

Das für die AEB gewünschte Qualitätsniveau bzw. unser eigener Qualitätsanspruch, der sich aus den generellen Kundenanforderungen und –Erwartungen ableitet, gibt die GL vor und manifestiert sich wie folgt:

AEB möchte…

- Lösungen einführen, die den Anforderungen unserer Kunden gerecht werden und sie begeistern.
- Durchgängige Software Produkte mit einer hohen Usability, die den Anforderungen des Marktes zu vertretbaren Preisen gerecht werden, einfach zu installieren, auszurollen und zu betreiben sind bieten.

- Durchgängige, zuverlässige Services (Service-Produkte), Erreichbarkeit und schnelles Reagieren im Emergency-Fall sowie ein zuverlässiges Facility Management (z.B. reibungsloser Betrieb des Rechenzentrums). Dabei gehen wir sicher und vertrauenswürdig mit Kundendaten und -wünschen um.
- Erfolgreiche und zufriedenstellende Projekte (Kundenprojekte u. interne Projekte) professionell und wirtschaftlich abwickeln. Stets im Bewusstsein das Unvorhergesehenes auftaucht und darauf flexibel reagiert werden muss. Dabei achten wir auch auf eine klare Rollen- und Aufgabenverteilung sowohl bei AEB als auch auf Kundenseite, um gemeinsam eine offene und kompetente Zusammenarbeit zu ermöglichen.
- Erfolgreiche, nachhaltige Vermarktung unserer Produkte und des Unternehmens.
  Dazu gehört eine seriöse, kompetente und transparente Kommunikation mit dem Markt und mit unseren Gesprächspartnern. Zuverlässigkeit und Nachvollziehbarkeit von Angebot bis Auftrag.
- Effiziente & transparente Verwaltung
  Eine effiziente und transparente Verwaltung, die die Einhaltung von gesetzlichen Vorschriften und Verträgen sicherstellt Schlanke Prozesse in der kaufmännischen Abwicklung in enger Verzahnung mit den Bereichen Verständlichkeit.
- Transparente und Vertrauenswürdige Mitarbeiterbetreuung, die mit Hilfe von Mitarbeiterverantwortlichen das Wohl und das optimale Wirken im Unternehmen eines jeden Einzelnen begleitet.
- Sicherstellung der Aus- und Weiterbildungsqualität, um Wissen und Kompetenz auf hohem Niveau zu halten.

Detaillierte Qualitätsziele

- Die Produkte und das Unternehmen erfolgreich und nachhaltig vermarkten
  Dies wird transparent durch:
  - Seriöse, kompetente, transparente Kommunikation mit dem Markt und mit unseren Gesprächspartnern
  - Zuverlässigkeit und Nachvollziehbarkeit von Angebot bis Auftrag
  - An hoher Servicequalität orientierte Vertriebsprozesse
  - Sicherer und vertrauenswürdiger Umgang mit Kundendaten
- Durchgängige Software Produkte zu entwickeln, mit einer hohen Usability, die den Anforderungen des Marktes zu vertretbaren Preisen gerecht werden, einfach zu installieren, auszurollen und zu betreiben sind.
  Dies wird transparent durch
  - Die Erfüllung fachlicher Anforderungen (Wettbewerbsfähigkeit der Softwarelösungen) und deren Aktualität (regelmäßige Updates)
  - Selbstverständliche und gebrauchstaugliche Software (freundlich, ergonomisch, intuitiv, erlebbar und leicht zu bedienen)
  - Fehlerfreiheit anstreben (jede Zeile Code wird abgenommen und getestet)

- Kompatibilität in der Systemlandschaft sicherstellen
- Einfache Installation gewährleisten
- Wartbarkeit und reibungsloser Betrieb sicherstellen

- **Lösungen einführen, die die Anforderungen unserer Kunden gerecht werden.**
  Dies wird transparent durch:
  - Integrierte und durchgängige Lösungen (Mix aus Software und Services)
  - Branchenspezifischen und kundenindividuellen Anpassungen, die effizient und nachvollziehbar gewartet werden können.
- **Durchgängige und umfassende Services (Service-Produkte) sowie zuverlässiges Facility und Application Management**
  Dies wird transparent durch:
  - Facility Management (z.B. reibungsloser Betrieb des Rechenzentrums)
  - Erreichbarkeit und schnelles Reagieren im Emergency-Fall
  - Datensicherheit und Datenschutz
  - Zuverlässige System-Technik
  - Schneller und kompetenter Kundensupport
  - Professionelles Training für Kunden
- **Erfolgreiche und zufriedenstellende professionelle Projekte durchführen (Kundenprojekte u. interne Projekte)**
  Dies wird transparent durch:
  - Professionelles Projekt Management
  - Wirtschaftlich effiziente Projekte durchführen
  - Klare Rollen- und Aufgabenverteilung auf AEB und Kundenseite
  - Bewusstsein, dass Unvorhergesehenes auftaucht, und die Fähigkeit, darauf flexibel zu reagieren
  - Offene und kompetente Zusammenarbeit
- **Effiziente und transparente Verwaltung, die die Einhaltung von gesetzlichen Vorschriften und Verträgen sicherstellt.**
  Dies wird transparent durch:
  - Die Einhaltung von Gesetzen, Vorschriften und Verträgen
  - Schlanke Prozesse in der kaufmännischen Abwicklung in enger Verzahnung mit den Bereichen
  - Verständlichkeit und Effizienz in der Kommunikation und in Verträgen
  - Schnelle Reaktionszeit bei Fragen und Reklamationen

- Sicherstellung der Aus- und Weiterbildungsqualität, um internes Wissen und Kompetenz auf hohem Niveau zu halten.

Qualitätspolitik

Die Qualitätspolitik der AEB basiert auf dem Unternehenshandbuch.
Im Wesentlichen sieht sich das QM dabei in in der folgenden Verantwortung bzw. verfolgt folgende Zielsetzung: Ziel ist es stets, unseren wertschöpfenden Geschäftsbetrieb bzw. –prozess sicherzustellen. D.h. unsere Service- und Softwareprodukt-Wertschöpfung muss reibungslos funktionieren, da sonst der Unternehmenserfolg gefährdet ist. Das QM sowie das QMS der AEB ist dazu auf die Mitarbeiter bzw. auf ihre Fähigkeiten und Rollen im Arbeitsalltag zugeschnitten und wird als Folge dessen durch sie stetig gelebt bzw. umgesetzt. Beides basiert auf einem durchgängigen Rollenkonzept, welches die Eigenverantwortung des einzelnen Mitarbeiters in der Wertschöpfung, im Unternehmenskontext fördert und stärkt.
QM wird von den Mitarbeitern selbst im Rahmen ihrer Rolle(n) betrieben – das QMS liefert dafür die entsprechenden Rahmenbedingungen.

AEB verfolgt damit folgende Grundsätze:

- Profis nehmen die Verantwortung für die (Ergebnis)Qualität in ihrer Arbeit täglich und gewissenhaft wahr.
- Das Erreichen der Qualität sowie das Betreiben von Qualitätsmanagement, ist die Verantwortung aller MA im Rahmen ihrer Arbeit bzw. ihrer Rolle(n) bei der AEB.
- Im Zuge dessen definieren die entsprechenden Rollen, Prozesse, Vorgaben und Tools und tragen für die kontinuierliche Aktualität sowie die inhaltliche Sinnhaftigkeit Verantwortung.
- Ein zentral synchronisiertes und verwaltetes QMS schafft die dafür nötigen Rahmendbedingungen und stellt entsprechende zentrale Tools zur Verfügung, um Synergien und Durchgängigkeit zu schaffen – trifft dabei jedoch keine inhaltlichen Entscheidungen und vermeidet die Kompensation der Mitarbeiterverantwortung.

Ziel ist es, **so viel wie nötig aber auch nur so wenig wie möglich** in Form von transparenten und gebrauchstauglichen Standards abzubilden. Es muss eine gesunde Balance entstehen zwischen Regelungen und Eigenverantwortung, damit die nötige Flexibilität erhalten bleibt, um auf besondere Anforderungen angemessen und kompetent reagieren zu können.
Wir unterscheiden daher zwischen **übergreifend gültigen Regeln (Themen)**, konkreten **Kernprozessen (sekundäre und primäre)**, ohne die unsere Wertschöpfung nicht effektiv stattfinden kann und zwischen **Begleitprozessen**, die eher dazu beitragen dass die einzelnen Arbeitsabläufe (z.B. innerhalb eines Teams oder in der Zusammenarbeit mit anderen einzelnen Teams) effizient sind.

2.2 Leitsätze zur Sicherheitsstrategie

Unsere maßgeblichen Sicherheitsziele sind **Verfügbarkeit, Vertraulichkeit und Integrität**. Die Sicherheitsziele und ihre Detaillierung unterliegen selber dem PDCA und sind in einem separaten Dokument zu finden.

Verfügbarkeit betrifft dabei nicht nur technische Aspekte der Erreichbarkeit unserer IT-Lösungen, sondern auch organisatorische Verfügbarkeit von Ansprechpartnern wie etwa für Support-Zwecke mit unseren Kunden. Diesbezügliche Vereinbarungen werden im Rahmen von Allgemeinen Geschäftsbedingungen, Standard-Verträgen oder gesondert in individuellen Vereinbarungen getroffen.

Vertraulichkeit betrifft nicht nur technische Belange wie etwa Zugriffsbeschränkungen entsprechend der Aufgabengebiete, sondern die Klarstellung und verpflichtende Vereinbarung von Befugnissen unserer Mitarbeiter im Umgang mit Daten insbesondere unserer Geschäftspartner.

Integrität fordert insbesondere klare Prozesse in der Informationsverarbeitung.

In Anlehnung an **COSO** wurde ein Internes Kontrollsystem (IKS) eingerichtet, um grundlegende Strategien und Prinzipien zu verankern wie:

- Anforderung nach Funktionstrennung
- 4-Augen-Prinzip für kritische Aktivitäten (Freigabe von Patches, Guides, Verträgen, Vergabe von Benutzerrechten…)
- Prinzip der Transparenz (Dokumentationspflichten)
- Regelungen zur Vertraulichkeit (u.a. Need-to-know-Prinzip)
- Einsatz von Risikomanagement (ISMS)

Grundsätzlich wollen wir als **Sicherheitsstrategie** das Prinzip verfolgen, Applikationen, Daten, Netze, Geräte und User jeweils individuell zu schützen. Dies stellen wir durch Technologien nach Stand der Technik und durch strukturiertes prozessgesteuertes Vorgehen sicher.

Für den Prozess der Risiko-Analyse wollen wir den Modell-Mix der ‚Sicherheit von innen nach außen' bzw. ‚Sicherheit durch Eigentümerschaft' befolgen. Grundsätzlich ist jede festgestellte (signifikante) Information ein schützenswertes Gut. Wir gehen daher den Weg der analytischen Vorgehensweise mit folgenden Charakteristiken:

- Inventarisierung der Informationen zum Anwendungsbereich (einschließlich tangierender Bereiche)
- Klare Zuordnung von Verantwortlichen zur Information
- Risikobetrachtung und Schutzmaßnahmen werden möglichst nahe zur Information entwickelt und in Einklang mit den Vorgaben dieser Policy gebracht.
- Kann dem Schutzbedürfnis einer Information durch Maßnahmen auf einer höheren Modellierungsebene wirkungsvoll Genüge getan werden, so haben diese Vorrang.
- Aus diesem Grunde ist die Inventarisierung so zu modellieren, dass der Betrieb des ISMS mit Sicherheitsmaßnahmen angemessen erfolgen kann.

Das ISMS hilft dabei zu größerer Handlungssicherheit. Dadurch wird auch der Prozess der Beschäftigung mit Risiken effizient gestalten.

Das ISMS ist dabei geeignet, die Sicherheitsziele zu erreichen und ist auch für die Perspektive Sicherheit Grundlage für ein verbindliches Wertesystem.

Das Verhältnis von Aufwand und Risikoreduktion soll für den entsprechenden Schutzbedarf des Anwendungsbereichs angemessen sein; entsprechend ist ein strategisches Risikomanagement installiert, das Maßnahmen an den Leitlinien ausrichtet und mit ihnen konform hält.

Das ISMS soll flexibel genug sein, sich ändernden Rahmenbedingungen oder Zielen anzupassen. Für die Nachhaltigkeit sorgt der kontinuierliche Betrieb.

Das ISMS ist auch ein Instrument zur Prävention und Problemvermeidung. Unsere Aktivitäten dazu umfassen unter anderem

- Diverse regelmäßige Kontrollen und interne und externe Audits. Um unsere Sicherheit zu prüfen, lassen wir uns regelmäßig intern und extern gezielt angreifen. Für die Durchführung dieser Penetrationstests beauftragen wir externen Dienstleister.
- Prinzip der Früherkennung (Monitoring und Alerting der Systeme)
- Nachbetrachtungen, Ursachen-Analysen (z.B. bei aufgetretenen Emergencies)
- Betrieb eines Notfall-Konzepts und einer Emergency-Organisation
- Durchführung von Notfall-Übungen (anhand simulierter Szenarien)
- Kontinuierliche Aktivitäten zur Security Awareness (Kampagnen, Schulungen, News, u.ä.)

Sicherheit - die wichtigsten Regeln

- Die AEB legt sich mit dem QM: Security Guide verbindliche Regeln auf, die von der Belegschaft getragen und beachtet werden. Hier nur einige Auszüge der wichtigsten Regeln als Überschriften:
- Für Sicherheit ist jeder MA mitverantwortlich; Security-Vorfälle werden über ein zentrales Werkzeug administriert.
- Regelungen zu Clean Desk; Sicherheit am Arbeitsplatz (u.a. Virenschutz)
- Sicherstellung der Sorgfaltspflichten durch Geheimhaltungserklärung
- Umgang mit Accounts und Passwörtern
- Umgang mit Daten außer Haus bzw. im Ausland
- Umgang mit Gästen
- Beachtung des Datenschutzes (intern und extern)
- Regelmäßige Teilnahme an Schulungsmaßnahmen (rund um Security Awareness)
- Sicherstellung zu Abschlüssen von Vertraulichkeitserklärungen mit unseren Geschäftspartnern bei Bedarf

3 Organisationsstrukturen im IMS

3.1 Rollen, Verantwortlichkeiten und Ressourcen

Einführung

Die Zustimmung des Managements zur ISMS-Leitlinie bedeutet auch die grundsätzliche Zustimmung des Managements dazu, welche identifizierten Risiken getragen werden.

Die AEB führt ein ausgeprägtes Rollenkonzept. Die aktuellen Instanzen und die Rolleninhaber können der Organisationsstruktur gemäß gültigen Organisationsdokumentation entnommen werden.

Eine Rollenbeschreibung umfasst Verantwortung, Aufgaben, Kompetenzen sowie Voraussetzungen, beteiligte Prozesse und Berechtigungen. Das Berechtigungskonzept ist an Rollen geknüpft. Jeder Mitarbeiter ist über ein einheitliches Instrument in der Lage, sich Auskunft über seine Rollen zu beschaffen.

Rollen im Securitykontext

Die relevanten Rollen sind:

Rolle	Funktion, Verantwortung	Mitglied in	Kommentar
Geschäftsführung	• Vorgebende Funktionen, somit auch hauptverantwortlich für die Wirksamkeit der Managementsysteme • Freigabe dieser Richtlinien • Freigabe der Organisation zum QMS und ISMS • Managementbewertung und -Review • Förderung der laufenden Verbesserung • Freigabe von Ressourcen und Mittel • Entscheidung über die Kriterien zur Akzeptanz von Risiken		Höchste Instanz der Verantwortung
ISMS Manager	• Verantwortlicher für den Betrieb des Managementsystems ISMS • Betrieb des PDCA-Zyklus zum Betrieb des ISMS • Leitung des IS-Boards • Controlling des ISMS gemäß unseren Vorgaben, insbesondere auch der Einhaltung regelmäßiger Aktivitäten • Veranlassung interner Audits • Erklärung der Anwendbarkeit erstellen	IS-Board; AK Security	

	• Dokumentation von Management-Änderungen • Sicherstellung Dokumentenlenkung • Wahrung der Kontakte zu Behörden und zu sicherheitsrelevanten Interessengruppen		
IT Security Manager	• Vermeidung von Risiken für das gesamte Unternehmen. • Koordinieren der sicherheitsrelevanten Rollen und Prozesse. • Hauptverantwortlich für den Security Guide. • Definiert unternehmenseinheitliche Informationssicherheitsstandards. • Stellt die Umsetzung und Einhaltung der Sicherheitsstandards sicher. • Koordiniert Sicherheitsanalysen. • Wahrung der Kontakte zu Behörden und zu sicherheitsrelevanten Interessengruppen	IS-Board; AK Security	
ISMS-Leitung (Sicherheits-management)	• Kontrolle der Arbeit am Risikobehandlungsplan • Beurteilung Wirksamkeit der Maßnahmen • Reporting Sicherheitsvorfälle • Schulungen zu Sicherheit und ISMS-Bewusstsein anbieten • Sicherheits-Checks veranlassen und überwachen	IS-Board	Die ISMS Leitung setzt sich aus den Rolleninhabern der ISMS Leitung und IT Security Manager
Domänen-Sicherheits-beauftragter	• Die Domänen-Sicherheitsbeauftragten sind für die Durchsetzung der relevanten Sicherheitsvorgaben in ihrer Domäne verantwortlich. Sie sind dazu verantwortlich für die Durchführung der Risikobetrachtung, einschließlich Risikobehandlung. Dazu beziehen sie für diesen Prozess bei Bedarf die jeweiligen Eigentümer der assets mit ein.	IS-Board	

	• Sie sind entsprechend u.a. für den Betrieb des ISMS geschult und eingearbeitet.		
Leitung IT	• IT-Infrastruktur • Betrieb des Rechenzentrums • Mit-Verantwortung zu BCM	AK Security	näheres im Service Guide definiert
AK Security	• Des Funktionieren der Security Organisation und das Reagieren auf Security Vorfälle		Siehe auch Domänen Sicherheitsbeauftragte r
SLA Manager	• Mitsprache bei Festlegung der tolerierten Risiken für Kunden-Installationen • Ist mit der Kenntnis der bestehenden SLAs und damit der vereinbarten Ansprüche der Kunden ausgestattet	AK Security	nur fallweise hinzugezogen
Datenschutzbeauftra gter (DSB)	• Hinwirken auf die Einhaltung des BDSG Wahrung der Kontakte zu Behörden und zu sicherheitsrelevanten Interessengruppen	AK Security	nur fallweise hinzugezogen
Compliance Officer	• Rechtskonformität • Monitoring auch von Änderungen von relevanten gesetzlichen Vorgaben	IS-Board	gemäß A.18

Domänen-Sicherheitsbeauftragte, Eigentümer und Verantwortung

- Für nachfolgend gelistete Domänen, die in direktem Zusammenhang mit unseren Haupt-Geschäftsprozessen stehen, konnten die so genannten Regelungsbereiche der ISO-Norm zugeordnet und die Rolle des **Domänen-Sicherheitsbeauftragten** eingerichtet werden.
- Die Domänen-Sicherheitsbeauftragten sind in ihrer Domäne verantwortlich für die Durchführung der Risikobetrachtung. Dazu beziehen sie für diesen Prozess die jeweiligen Eigentümer der assets mit ein.
- Details und Detail-Zuordnungen regelt eine interne Dokumentation. Dort wird für jedes Kontrollziel ein Verantwortlicher zugeordnet. Die Domänen-Sicherheitsbeauftragten berücksichtigen daher regelmäßig diese Dokumentation für ihren Wirkungsbereich zu ihrer Zuständigkeit und Verwirklichung des Maßnahmenziels.

Nr.	Domäne
1	**Verwaltung** mit Themen zu • Recht und Gesetz, Compliance, Datenschutz • Kaufm. Abwicklung, Controlling, Buchhaltung
2	**Mitarbeiterbetreuung** (Personal/HR)

3	**Infrastruktur** mit Themen zu • Haustechnik • Hausservice
4	**IT** mit Themen zu • Systemmanagement • Rechenzentrum
5	**Services** mit Themen zu • Support
6	**Produkte** / Technik zur Anwendung
7	**Lösungen** (Kundenprojekte)
8	**Vertrieb/Vermarktung**

Die genauere Zuständigkeit wird im *IS-Board unter Regelungsbereiche* verdeutlicht.

QM Verantwortung

Das QM wird - wie bereits in seiner Definition erwähnt - vor allem durch die Mitarbeiter selbst im Rahmen ihrer Rolle(n) betrieben. Dazu ist in den jeweiligen Rollen die Verantwortung für die Ergebnisqualität entsprechend des von der GL vorgegebenen Qualitätsanspruchs definiert.

Details finden sich dazu in den jeweiligen Rollenbeschreibungen sowie in dem Rollenkonzept der AEB
Das QM wird von den jeweiligen Rollen gemäß dem PDCA-Zyklus:

- geplant (bedarf es überhaupt eines geregelten Prozesses, Regeln und/oder Tools zur Vorgehensweise?)
- aufgesetzt (handelt es sich um einen Kern- oder eher Begleitprozess)
- eingeführt (kommuniziert, geschult, dokumentiert, getestet)
- umgesetzt bzw. gelebt
- kontinuierlich verbessert und gepflegt (z.B. durch regelmäßige Beauftragung interner Audits und durch PDCA-Kreislauf).

Das QMS schafft – wie bereits in seiner Definition erwähnt – die nötigen Rahmenbedingungen für die Kernprozesse des QMs. Dazu wird es von Mitarbeitern in der Rolle des QMS Verantwortlichen gemeinsam zentral verwaltet und allen Mitarbeitern zur Verfügung gestellt. Sie begleiten/coachen und fördern andere Mitarbeiter, die im Rahmen ihrer Rolle(n), Verfahren und Qualitätssichernde Maßnahmen, Tools, Schulungen etc. festlegen wollen. Durch regelmäßigen Austausch zwischen einander sorgen sie so automatisch für einen transparenten Überblick und eine einheitliche Dokumentation der wertschöpfenden Kernprozesse. Sie schulen bzw. vermitteln das „System“ sowohl intern als auch nach außen (z.B. im Rahmen von Ausschreibungen oder externen Kunden-Audits). Sie überprüfen das System regelmäßig auf Angemessenheit bezogen auf den geforderten Qualitätsanspruch z.B. durch interne Audits oder durch das „Finger in die Wunde legen“ bei auftretenden Widersprüchen. Sie unterstützen im Zuge dessen moderierend, treffen jedoch keine Entscheidungen – fordern diese aber kontinuierlich von den entsprechenden Verantwortlichen ein.

Darüber hinaus betreiben die Kernprozess- und Themenverantwortliche Qualitätsmanagement für den zugeordneten Kernprozess/-Thema. Im Zuge dessen bündeln bzw. synchronisieren und orchestrieren sie die betroffenen Beteiligten/Rollen, um die Erreichung des für unseren Geschäftserfolg notwendigen Qualitätsanspruchs sicherzustellen. Sie stehen bzgl. QM in direkter Abstimmung mit den QMS Verantwortlichen.

3.2 Administration

Zur Pflege des Managementsystems und Wahrung aller zugehörigen Aktivitäten werden Aufgaben und Mittel (Aufwände) als Projekte im Tool ASSIST4CRM verwaltet. Diese Projekte haben folgende Charakteristik

- jeweils eine Laufzeit von 1 Jahr.
- Sie weisen Rollen aus; zumindest immer Projektleiter, -Manager.
- Veranschlagter Aufwand

Die benötigten Mittel werden regelmäßig ermittelt und bereitgestellt. Bei Bedarf wird korrigiert. Diese Leitlinie wird als im unternehmenseigenen WIKI veröffentlicht und per NEWS vermittelt.

Zur regelmäßigen Prüfung dieser Leitlinie dienen

- interne (regelmäßige) Audits
- Ereignisse, die das Anwendungssystem oder relevante Randbedingungen verändern.

3.3 Kompetenz und Bewusstsein

Verantwortung und Kompetenz sind zentrale Elemente in den Rollenbeschreibungen der AEB. Die Zuordnung von Personen zu Rollen ist ein gemanagter Prozess. Auch die Rollenbeschreibungen unterliegen einem gemanagten Prozess mit Rollen-Verantwortlichen und 4-Augen-Prinzip für die Rollen-Freigabe. Allen Rollen steht ein Recht auf angemessene Aus- und Weiterbildung zu. Die Organisation und ihre Kultur stellen sicher, dass Kompetenz im Sinne von Erfahrung sich im Netzwerk entfalten kann.

- Wichtige Elemente sind die Kenntnis und der vertraute Umgang mit
- den Zielen (u.a. in den Leitlinien)
- den Prozessen und Abläufen zur Erreichung der Ziele
- den dabei vorgesehenen Werkzeugen incl. Dokumentationen

Kommunikation findet in Form von Gesprächen, Meetings, Schulungen oder im Rahmen einer Dokumentenlenkung (etwa per NEWS) statt. Dabei wird die Bedeutung der Beachtung bzw. Nicht-Beachtung der Leitlinien der AEB vermittelt. Und es wird betont, dass jeder Beitrag/jede Beteiligung eines jeden Mitarbeiters wichtig ist für den gemeinsamen Erfolg ist.

3.4 Kommunikation

Ein lebendes Managementsystem erfordert Kommunikation. Mit Blick auf Qualitätssicherung ist gemäß folgendem Grob-Schema aktiv zu informieren:

wann (Anlass)	was	wer	wem	wie
Änderung von Vorgaben	Inhalte der Änderung, Gründe	Wächter der Vorgabe (z.B. GF, QM)	QMS Verantwortliche, betroffene Mitarbeiter	Mail (und Meeting); Dokumentation in Korrektur- und Vorbeugemaßnahmen
Änderung der Organisation	Inhalte der Änderung, Gründe	Leiter der Organisation	QMS Verantwortliche, betroffene Mitarbeiter	Mail, NEWS, bei Bedarf Nachschulung
Änderung an Guides	Inhalte der Änderung, Gründe	Verantwortlicher des Guides	Belegschaft oder betroffen Domäne, entsprechende Zielgruppe	NEWS, bei Bedarf Nachschulung

Im Firmeneigenen Intranet (WIKI) werden Informationen transparent zur Verfügung gestellt. NEWS nehmen häufig zu weiteren Ausführungen Bezug auf WIKI.

3.5 Dokumentierte Informationen

Allgemeines

Die Organisation hat zur Beachtung genereller Dokumentationsanforderungen eine Richtlinie zur Dokumentation erstellt. siehe *QM: Regeln zur QM-Dokumentation*. Das Einrichten und Führen eines Managementsystems bedeutet die regelmäßige Durchführung gemäß eines PDCA-Zyklus; hierzu gehören mindestens folgende zu dokumentierende Aktivitäten:

- regelmäßige Begutachtung und weiterführende Pflege der für das Managementsystem erforderlichen Dokumentationen
- Schulungen zur Aus- und Weiterbildung werden in der AEB als „Bausteine“ bezeichnet. Pflichtbausteine gehören zur Grundausbildung (GA) und müssen von jedem neuen Mitarbeiter besucht werden. Als Pflichtbausteine eingestuft sind z.B. aufgrund ihres hohen Stellenwerts Schulungen zur Sicherheit (Arbeitsschutz, Datenschutz, Datensicherheit, ISMS). Nähere Informationen findet man im Wiki in der *Kategorie: Weiterbildung*.
- Die Audits – auch die internen - werden protokolliert.

Weitere regelmäßige Aktivitäten

im QMS

- Aktualisierung aller Regeln und Prinzipien (1x / Jahr)
- Aktualisierung der Wertschöpfungskette und aller hinterlegten Prozesse inkl. Rollen (1x / Jahr)
- Interner Audit des QMS nach Beauftragung der Prozessverantwortlichen

im ISMS

- Wiederholung der Risikoeinschätzung; mindestens 1 x / Jahr
- Pflege des Risikobehandlungsplans
- Pflege der Korrektur- und Vorbeugemaßnahmen
- Erklärung zur Anwendbarkeit (Überprüfung auf Aktualität)
- Regelmäßiges Durchführen einer Managementbewertung
- Internes Audit des ISMS

4 PDCA im IMS

4.1 Führung

Führung und Engagement

Aus dem Selbstverständnis der AEB und wie wir agieren wollen und wie wir auf dem Markt auftreten leitet sich unser hoher Anspruch an Qualität und Sicherheit ab. Die Geschäftsführung legt hierauf besonderen Wert und versteht sich in der Verantwortung für Qualitätsmanagement und Sicherheit. Die Geschäftsführung möchte, dass allen Mitarbeitern die besondere Verantwortung und Sorgfaltspflicht hierfür klar ist und sie entsprechend handeln.

Dazu hat sie Managementsysteme für Qualität und Sicherheit etabliert, die den folgenden Kriterien entsprechen:

- konform zu den entsprechenden ISO-Normen
- in die Organisation strategisch integriert
- prozessorientiert zur kontinuierlichen Verbesserung ausgerichtet, um die Qualitäts- und Sicherheitsziele zu erfüllen

Die dafür notwendigen Aufwände und zusätzlichen Ressourcen werden bereitgestellt. Entsprechende Rollen haben u.a. auch Controlling-Verantwortung. Wichtiger Aspekt des Führungsauftrags neben der Ausrichtung auf die Ziele ist die Förderung aller Beteiligten, kontinuierlich einen Beitrag zur tatsächlichen Wirksamkeit und zur steten Verbesserung zu leisten.

Leitlinien zu Managementsystemen

Wesentlicher Teil der beteiligten Managementsysteme sind die zugehörigen Leitlinien. Diese erfüllen folgende Kriterien:

- konform zu den entsprechenden ISO-Normen
- Darstellung der Zielsetzung und ihrer Begründung
- Darstellung der Anwendungsbereiche, auf die die Managementsysteme ausgerichtet sind
- Darstellung der Organisation, die mit der Umsetzung der Ziele betraut wird.

Diese Leitlinien unterliegen den Prozessen für Richtliniendokumente. Sie werden schriftlich abgefasst und ihre aktuellen Versionen den Mitarbeitern zur Beachtung verfügbar gemacht.

Organisatorische Aufgaben, Zuständigkeiten und Befugnisse

Wichtiger Bestandteil in den Leitlinien ist die Klarstellung der Organisation mit Rollen und ihren Funktionen und Befugnissen. Ziel der Organisation ist die kontinuierliche Ausrichtung an den in der Leitlinie verankerten Zielsetzung sowie auch deren Weiterentwicklung und Anpassung an veränderte Rahmenbedingungen. Dazu ist in den Managementsystemen ein Rückschluss verankert; im Rahmen von regelmäßigen Managementbewertungen wird Bericht erstattet und werden anstehende Korrektur- und Vorbeugemaßnahmen beschlossen und ergriffen.

4.2 Umgang mit Risiken und Chancen

Wo Ziele sind, sind auch Rahmenbedingungen, die die Zielerreichung gefährden oder begünstigen können. Gerade die ausdrückliche Betrachtung von Risiken und Chancen ist ein wichtiges Instrument, die Zuverlässigkeit in der Zielerreichung zu erhöhen. Diese Betrachtung ermöglicht die Konzentration auf die eigentlichen Geschäftsziele.

Betrachtungen im Umfeld des ISMS

Ausgehend von den Leitsätzen der Informationssicherheitsleitlinie betreibt die AEB ein ISMS, in dem laufend Sicherheitsrisiken identifiziert und nach einer Schutzbedarfsanalyse bewertet werden. Vor einer möglichen Risikobehandlung wird in der regelmäßig einberufenen Managementbewertung über die angemessene Vorgehensweise entschieden. Das Nähere, wie etwa die Prozesse zur Risikoeinschätzung und -behandlung, ist in einem ISMS-Richtliniendokument der AEB geregelt; näher beschrieben im QM:ISMS Guide.

Betrachtungen im Umfeld des QMS

Im Umfeld des Qualitätsmanagements sind Risiko und Chance noch mehr zwei Seiten der gleichen Medaille. Tiefes Bewusstsein über die Qualitätsziele schärft das Interesse, sie zu erreichen. Tiefes Bewusstsein in mögliche Risiken, die das Erreichen der Qualitätsziele verhindern oder beeinträchtigen könnten, hilft, entsprechende Vorkehrungen zu treffen, um mit größerer Zuverlässigkeit die Ziele zu erreichen. Im gleichen Verständnis erhöht diese Betrachtung die Chance der Zielerreichung. Zusätzlich bietet das Betreiben von Risikomanagement im QMS die Chance auf der Ebene von Vertrauen in Zuverlässigkeit und Qualität am Markt.

4.3 Planung von Veränderungen

Durch regelmäßige interne Audits überprüfen wir sowohl das QMS als auch das ISMS 1x jährlich auf Gebrauchstauglichkeit, Aktualität und Einhaltung. Alle Informationen, wie interne Audits in der AEB durchgeführt werden, sind hier zu finden und definiert:

Zertifikate

Auf der Wiki Seite *Zertifikate* sind alle Zertifikate der AEB zu finden. Auf der AEB Webseite sind auf der *Service-Seite* alle Zertifikate zu finden, wie wir sie auch extern bereitstellen.

QM-gesteuerte Veränderungen

Das Qualitätsmanagement orientiert sich im Rahmen seiner Arbeit am sogenannten Demingkreis oder besser als „PDCA-Zyklus“ bekannt. Dieser beschreibt einen iterativen vierphasigen Problemlösungsprozess als Systematik zur kontinuierlichen Verbesserung. PDCA steht gem. der Theorie hierbei für Plan–Do–Check–Act und basiert auf dem Gemba-Prinzip. Das Gemba-Prinzip bedeutet "Gehe an den Ort des Geschehens" an dem wertschöpfende Prozesse im Unternehmen stattfinden und an dem die Probleme auftauchen, um vor allem die Mitarbeiter vor Ort mit ihrer exakten Kenntnis der Situation in den Mittelpunkt der Planung zu stellen.

PDCA, PDCA-Zyklus oder PDCA-Regelkreis ist also…

- ein Grundprinzip eines Managementsystems (für Querschnittsfunktionen wie Qualität oder Sicherheit)
- und steht für: "Plan-, Do-, Check-, Act-Zyklus"

Dieses Prinzip verwenden wir daher in

- unserem Qualitätsmanagement (QMS)
- unserem Informationssicherheitsmanagement (ISMS)

Siehe dazu auch *QM Methoden & Standards.*

Dazu gehört auch:

- Änderungen an der IT-Landschaft, den Geschäftsprozessen oder Bedrohungen oder deren Einschätzung müssen zur Neubetrachtung der inhaltlichen Richtigkeit und Sinnhaftigkeit führen.
- Änderungen von Regelungen und gesetzlichen Vorgaben
  - In besonderer Bringschuld stehen hier unsere Rollen Compliance Officer, Datenschutzbeauftragter und das Team Recht.
  - Generell gilt zusätzlich: Sollten gesetzliche Anforderungen auf anderen Wegen (z.B. IHK Bekanntmachungen oder Informationsrecherchen) einem Mitarbeiter bekannt werden, so sind diese

als Servicefälle an Recht oder AK Security in den Regelprozess zu bringen. Bei Bedarf werden diese Fälle im IS-Board weiter erörtert.

- Veränderungen werden bewusst, begründet und nachvollziehbar herbeigeführt.

4.4 Bedeutung des Wissensmanagement für das IMS

Wissen zu bewahren und aufzubauen, strukturiert zu verteilen und wiederzufinden, ist für Unternehmen mit verteilten Standorten in unterschiedlichen Ländern eine dauerhafte Herausforderung. Dieser stellen wir uns mit gut organisierten Kommunikationswegen und Ablagesystemen, zusätzlich zum persönlichen Kontakt direkt, telefonisch oder per Mail.

Intern hilft uns dabei ein zweisprachig aufgebautes Intranet mit Wiki-System, über das schnell News verbreitet und Wissen für andere zur Verfügung gestellt werden können. Nach außen pflegen wir verschiedene Pfade zum Kunden: Über unsere Homepage www.aeb.com können sich Interessenten und Kunden über unser (weiteres) Angebot informieren, per Newsletter, in der Community und im Kundenportal werden aktuelle Themen bekannt gegeben und zur Diskussion gestellt.

- Mehr Details zum Wissensmanagement: *QM:Wissensmanagement*

4.5 Operativer Betrieb / Einsatz

Die Vorgaben der Leitlinien sind auszugestalten und umzusetzen. Als Anforderungen für diese Umsetzung sind zu beachten:

- weiterführende Dokumentationen zur Umsetzung unterliegen ebenfalls den QM-Richtlinien
- diese Dokumentationen sind transparent und erbringen den Nachweis, die Vorgaben umzusetzen (Nachvollziehbarkeit, Stimmigkeit)
- Kontrolle und Dokumentation von Änderungen

ISMS

- Zur Umsetzung dieser Leitlinie für die Informationssicherheit steht ein *QM: ISMS Guide* zur Verfügung. Dieser regelt u.a. die regelmäßige
- Risikoeinschätzung
- Risikobehandlung

QMS

- Die Umsetzung des QMS wird auf dieser Seite *QM:Qualitätsmanagement* ausführlich erläutert. Für einen kurzen Auszug auch zu Durchsetzungsmaßnahmen siehe Abschnitt *Qualitätspolitik*.

4.6 Sicherstellung von Kontrolle und Wirksamkeitsmessung

Fragestellung/Ziel: Wodurch stellen wir sicher, dass wir die Anforderungen im Blick behalten, die an das jeweilige Managementsystem gestellt werden?

Die Leitlinie zum Managementsystem stellt Organisation und Rollen dar, die im Managementsystem entsprechende Befugnisse und kontrollierende Verantwortung tragen. Die Sicherstellung der Wirksamkeit sorgt für den Brückenschlag zwischen Wille und realem Geschehen, um die Zielerreichung zu fördern. Diesen Brückenschlag vorzunehmen ist Teil der Selbstverpflichtung der Führung. Zusätzlich beinhalten die Prozesse und Werkzeuge selbst eingebettete Kontrollen, die zur Sicherstellung der Ziele unter Einbeziehung der Zielkriterien führen. Beispiel: Für die Betreuung von Partnerschaften (Dienstleister, Lieferanten, Partner für Entwicklung, Vertriebspartner) stellen wir Mitarbeiter mit der dedizierten Rolle des Partnermanagers während des gesamten Lifecycles zur Verfügung.

Zur Sicherstellung der Wirksamkeit der Qualitätsmaßnahmen dienen ferner folgende Instrumente:

Instrument	Beteiligte Rollen	Indikatoren und Messlatte in der Wirksamkeitsprüfung
Durchführung auch der Dauerläufer-Aufgaben Qualität und Sicherheit als Projekte mit Maßnahmenpaketen, mit Zuordnung der Verantwortung, …	Projektmanager, Projektleiter, Projekt-Mitarbeiter	RFT (Blick auf Ressource, Funktion, Termin); Kontroll-Termine mit Projektmanager, ggf. PEM durchführen
bei komplexeren oder herausfordernden Projekten auch Projekt-Meetings bei Auftakt und Ende; Einflussnahme auf Projekt-Charakteristik; Arbeiten in Meilensteinen	Projekt-Team, Geschäftsführung	auch RFT; Betrachtung Chancen und Risiken
Arbeiten mit Termin-Serien mit Agenda zu Aufgaben-Raster	Termin-Organisator, Teilnehmer	Feedback-Kultur (Beteiligung, Anzahl und Inhalte der Feedbacks)
Auswertungsmeetings zu KPI; auch zur Vorlage und Diskussion in Managementbewertung; strukturierter Aufbau zu Managementbewertungen, der auch selbst regelmäßig auf Eignung abgestimmt wird	Leitung Managementsystem, Top-Management	jeweilige KPI-Liste; Abfragen; Statistische Auswertung zu Trend
In Weiterbildungsprogramm integrierte Feedbacks	Weiterbildung, Trainer	offenes, anonymes, nicht geführtes Feedback (liefert in der Regel Aussagen zu Zufriedenheit, Verständlichkeit, Bewusstsein zu transportierten Inhalten)
interne und externe Audits	Auditoren, Prozess-Beteiligte,	Vorgaben der Richtlinien-Dokumente zu Managementsystem; Feedback-Runden; Qualität des internen Audit Guides, der auch Einholen von Feedbacks vorsieht.

gelenkte Kommunikation	Autoren	Vorgaben, u.a. Richtlinien-Dokumente, Verwendungshinweise
integriertes Risikomanagement	Projektleiter, Projektmanager, ISMS Manager	Checklisten zur Anregung, über Risiken nachzudenken, die die Ziele gefährden könnten
Risikobehandlung	Domänen-Sicherheitsbeauftragte, Risiko-Eigentümer	Abschnitt innerhalb Risikobehandlung integriert. Darin Indikator(en) festzulegen, die das Auftreten des Risikos zum Ausdruck bringen. Beispiel: Anzahl Servicefälle mit def. Symptom.
Kunden-Befragungen, Feedback einholen	Marketing, Service-Organisation	Aktion-getriebene Fragebögen; Auswertung

4.7 Verbesserung

Die letzte Phase Verbesserung schließt den Kreislauf zum geregelten iterativen Prozess, indem Erkenntnisse im Betrieb des Managementsystems umgesetzt werden und dabei auch die Vorgaben korrigieren können.

Entsprechende Erkenntnisse müssen daher

- dokumentiert und analysiert,
- auf Gründe zu z.B. Fehlerursachen untersucht,
- zu Ideen für Korrektur- oder Vorbeugemaßnahmen entwickelt

werden.

Die Korrektur- und Vorbeugemaßnahmen sind ihrerseits

- zu dokumentieren
- in Anpassungen der Vorgaben zu überführen
- den Betroffenen zuzuführen

Weitere wesentliche Dokumente

- *QM: Security Guide*
- *QM: ISMS Guide*
- *QM: Qualitätsmanagement*