

Leitlinie

Integriertes Management System (IMS)

30.08.2024

www.aeb.com

AEB

A large, colorful, triangular graphic element in the bottom right corner of the page. It features a gradient of colors including purple, blue, green, yellow, and orange, forming a large triangle that points towards the top right.

Inhalt

1	Leitlinie und Regeln zur Politik von Informationssicherheit, Datenschutz und Qualität	1
1.1	Zweck und grundsätzlicher Anspruch	2
1.2	Vorgaben und Anforderungen	2
1.2.1	Geschäftserfordernisse	3
1.2.2	Gesetzliche Anforderungen	4
1.2.3	Vertragliche Anforderungen	4
1.2.4	Sonstige regulative Anforderungen	5
1.3	Anwendungsbereiche	5
1.3.1	Zur ISO 9001 – Verfahren und Prozesse	5
1.3.2	Begründung für die Auswahl	5
1.3.3	Zur ISO 27001 – Verfahren und Prozesse	5
1.3.4	Begründung für die Auswahl	6
1.3.5	Zur ISO 27018 – Verfahren und Prozesse	6
1.3.6	Begründung für die Auswahl	6
2	Die Managementsysteme QMS, DSMS und ISMS im IMS	6
2.1	Leitsätze zur Qualitätspolitik	7
2.1.1	AEB-Qualitätsanspruch	7
2.1.2	Detaillierte Qualitätsziele	7
2.1.3	Qualitätspolitik	9
2.2	Leitsätze zur Sicherheitsstrategie	9
2.2.1	Sicherheit – die wichtigsten Regeln	11
2.3	Leitsätze zum Datenschutz	11
3	Organisationsstrukturen im IMS	12
3.1	Rollen, Verantwortlichkeiten und Ressourcen	12

3.1.1	Einführung	12
3.1.2	Rollen im Security- und Datenschutzkontext	12
3.1.3	Domänen-Sicherheitsbeauftragte, Eigentümer und Verantwortung	14
3.1.4	QM Verantwortung	15
3.2	Administration	16
3.3	Kompetenz und Bewusstsein	16
3.4	Kommunikation	17
3.5	Dokumentierte Informationen	17
3.5.1	Allgemeines	17
3.5.2	Weitere regelmäßige Aktivitäten	18
4	PDCA im IMS	18
4.1	Führung	18
4.1.1	Führung und Engagement	18
4.1.2	Leitlinien zu Managementsystemen	19
4.1.3	Organisatorische Aufgaben, Zuständigkeiten und Befugnisse	19
4.2	Umgang mit Risiken und Chancen	19
4.2.1	Betrachtungen im Umfeld des ISMS	19
4.2.2	Betrachtungen im Umfeld des QMS	20
4.2.3	Betrachtungen im Umfeld des DSMS	20
4.3	Planung von Veränderungen	20
4.3.1	Zertifikate	20
4.3.2	QM-gesteuerte Veränderungen	20
4.4	Bedeutung des Wissensmanagements für das IMS	21
4.5	Operativer Betrieb / Einsatz	22
4.5.1	ISMS	22
4.5.2	QMS	22
4.5.3	DSMS	22
4.6	Sicherstellung von Kontrolle und Wirksamkeitsmessung	22

4.7	Verbesserung	24
4.7.1	Weitere wesentliche Dokumente	24

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

1 Leitlinie und Regeln zur Politik von Informationssicherheit, Datenschutz und Qualität

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 ISO-Normen ISO 9001, ISO 27018 und ISO 27001.

Dabei werden in dieser Leitlinie folgende Kapitel bedient:

Kapitel der ISO-Norm	Inhalte, Zwecke	Hier zu finden in
4 – Umfeld der Organisation	<ul style="list-style-type: none">• Verständnis der Organisation• Interessierte Parteien und ihre Erwartungen• Anwendungsbereiche zu Qualitätsmanagementsystem bzw. Informationssicherheitsmanagementsystem	<ul style="list-style-type: none">• Abschnitt 1.2• Abschnitt 1.2• Abschnitt 1.3
5 – Führung(sverhalten)	<ul style="list-style-type: none">• Führung und Selbstverpflichtung• Qualitätspolitik• Aufgaben, Verantwortung, Befugnis	<ul style="list-style-type: none">• Abs. 1.1, Abs. 4.1.1• Abschnitt 2.1• Abschnitt 4.1.3
6 – Planung	<ul style="list-style-type: none">• (Umgang mit) Risiken und Chancen• Qualitätsziele• Planung von Veränderungen	<ul style="list-style-type: none">• Abschnitt 4.2• Abschnitt 2.1• Abschnitt 4.3
7 – Unterstützung	<ul style="list-style-type: none">• Ressourcen• Kompetenz• Bewusstsein• Kommunikation• Dokumentierte Informationen	<ul style="list-style-type: none">• 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 Sicherheit, Qualität und Datenschutz
- 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-Normen.

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, Datenschutz und Sicherheit zusammen darzustellen, spezielle Aussagen zu Qualität, Datenschutz 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 zu Qualität, Datenschutz und Informationssicherheit (Rahmen zum Setzen von Zielen, Handlungsgrundsätze u. ä.). Eine wesentliche Orientierung bieten z.B. die ISO 9001, ISO 27018 und die ISO 27001. Für die ISO-Norm 27001 sind wir seit Februar 2010 zertifiziert.

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



1.2 Vorgaben und Anforderungen

Ziel: Welche Vorgaben welcher interessierten 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; Erwartungen zur Business Continuity	Allgemeine Geschäftsbedingungen (AGB); Vertragliche Bindung (Lizenz, Support, SLA, NDA, ...); Aussagen in Leistungsbeschreibungen	Produktmanagement, Recht, Services-Organisation (u. a. SLA-Management) Pflege und Kontrolle der Sicherheitsmaßnahmen

Partei	Interessen	Schnittstellen	Wie im Griff?
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
Versicherungen	Einhaltung der vertraglichen Bedingungen	Verträge mit Versicherungsumfang	Regelmäßiger Austausch und Review
Mitarbeitende	Gesundheitsumfeld; gute klimatische Atmosphäre; ethische Korrektheit	Arbeitssicherheit; einvernehmliche Kultur	Ständiger Austausch; Sensibilisierung; Code of Conduct; Leitlinien

Weitere Ausführungen:

1.2.1 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 Cloud-Lösungen auch angehalten, die Sicherheits-, Datenschutz- und Qualitätsansprüche zu erfüllen, die sich z. B. aus gesetzlichen Anforderungen für unsere Kunden und deren Prozesse ergeben. Die Einhaltung von Datenschutz- und 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 und Services ab.

Die AEB nimmt die Perspektiven Datenschutz und Sicherheit als zunehmend wichtiges Entscheidungskriterium im Markt wahr. Diese Perspektiven beschränken 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.

Klimawandel ist für AEB ein relevantes Thema. AEB hat diesen Aspekt mit Betrieb unseres ISO-zertifizierten ISMS in der Risikobetrachtung integriert. Bedrohungen der höheren Gewalt (wie Stürme, Hochwasser, große Hitze) sind dabei Gegenstand regelmäßiger Betrachtung und Einschätzung.

Als Chance betrachten wir, aus innerem ethischen Anspruch und Gefühl der Mitverantwortung heraus einen Beitrag zu leisten, sowohl eigene Beiträge zur Drosselung des Klimawandels zu leisten als auch unsere Resilienz gegen Auswirkungen des Klimawandels zu zeigen und so unsere Kunden-Services zu schützen und uns gewissenhaft zu engagieren.

1.2.2 Gesetzliche Anforderungen

Die Liste einschlägiger Gesetze und Vorgaben wird regelmäßig auf Relevanz geprüft. Dies umfasst insbesondere:

- KonTraG (Maßgabe, ein Überwachungssystem einzurichten; Früherkennung; Aussagen über Risikostruktur; Nachweis der Nachvollziehbarkeit über die Funktion eines Kontrollsystems)
- GDPdU, GoBD, GoBS (Sorgfaltspflichten bei der Verarbeitung, Vorhaltung und Bereitstellung von Informationen, insbesondere zu rechnungsrelevanten Daten zur Buchführung und Steuerprüfung; Forderung zur Einrichtung eines internen Kontrollsystems IKS)
- DS-GVO, BDSG (Datenschutz, Bereitstellung eines Sicherheitskonzepts nach Art. 32 DS-GVO – techn. und organisatorische Maßnahmen; Sorgfalt hinsichtlich Persönlichkeitsrechten Betroffener, Datensparsamkeit, Vertraulichkeit, Zweckgebundenheit, usw.)
- TKG, DDG, TDDDG (Telekommunikation und Telemedien)
- IT-Sicherheitsgesetz (NIS-Richtlinie, KRITIS, mit Bedeutung für kritische Infrastrukturen)
- 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 AWW, Dual-Use, Embargolisten. Somit sind auch Ämter wie das BAFA (Bundesamt für Wirtschaft und Ausfuhrkontrolle) wichtige Quellen.

1.2.3 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 DS-GVO gibt uns Vorschriften vor, die uns im Umgang mit unseren Kunden, Partnern und Subunternehmern zu besonderen Sorgfaltspflichten 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.

1.2.4 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 Verantwortlichen kontinuierlich überwacht
- und regelmäßig im Rahmen von internen Audits geprüft

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

- ist ein PDCA-Zyklus aufgesetzt, aus dem auch Verantwortlichkeiten und Spielregeln hervorgehen (s.u.)
- 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, ISO 27018 und ISO 27001 und den zugehörigen Managementsystemen

1.3 Anwendungsbereiche

1.3.1 Zur ISO 9001 – Verfahren und Prozesse

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

- alle Standorte
- alle Produkte

1.3.2 Begründung für die Auswahl

Mit der Bedeutung von Cloud-Angeboten und Dienstleistungen in wertschöpfenden Prozessen von Unternehmen (AEB Kunden) steht deren Anspruch an die Qualität der AEB Angebote im Fokus. AEB ist es wichtig, die Kunden mit Standard Cloud-Angeboten, individuellen Lösungen und Services zu überzeugen, die auch langfristig die an sie gehegten Erwartungen erfüllen und dabei höchsten Qualitätsansprüchen genügen.

1.3.3 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

1.3.4 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

1.3.5 Zur ISO 27018 – Verfahren und Prozesse

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

- alle Personen
- alle Standorte
- alle Produkte
- alle Kunden

1.3.6 Begründung für die Auswahl

- Eine Einschränkung des Scopes ist hier weder vorgesehen noch sinnvoll

2 Die Managementsysteme QMS, DSMS 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

2.1.1 AEB-Qualitätsanspruch

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

AEB möchte

- Lösungen einführen, die den Anforderungen unserer Kunden gerecht werden und sie begeistern.
- Durchgängige Cloud-Angebote (Standard-Softwareprodukte) mit einer hohen Usability bieten, die den Anforderungen des Marktes zu vertretbaren Preisen gerecht werden und zuverlässig zu betreiben sind.
- Durchgängige, zuverlässige Services (Serviceprodukte), 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 und interne Projekte) professionell und wirtschaftlich abwickeln. Stets im Bewusstsein das Unvorhergesehene auftaucht und darauf flexibel reagiert werden muss. Dabei achten wir auch auf eine klare Rollen- und Aufgabenverteilung sowohl bei AEB als auch auf Kundenseite. Dies soll gemeinsam eine offene und kompetente Zusammenarbeit ermöglichen.
- Eine 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.
- 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.
- Eine transparente und vertrauenswürdige Mitarbeiterbetreuung, die 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.

2.1.2 Detaillierte Qualitätsziele

- Die Cloud-Angebote 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 Vermarktungsprozesse

- Sicherer und vertrauenswürdiger Umgang mit Kundendaten
- Entwicklung durchgängiger Cloud-Angebote mit einer hohen Usability, die den Anforderungen des Marktes zu vertretbaren Preisen gerecht werden und zuverlässig zu betreiben sind. Dies wird transparent durch:
 - Die Erfüllung fachlicher Anforderungen (Wettbewerbsfähigkeit der Softwarelösungen) und deren Aktualität (regelmäßige Updates)
 - Selbstverständliche und gebrauchstaugliche Cloud-Angebote (freundlich, ergonomisch, intuitiv, erlebbar und leicht zu bedienen)
 - Fehlerfreiheit anstreben (jeder Code wird abgenommen und getestet)
 - Wartbarkeit und reibungsloser Betrieb sicherstellen
- Einführung von Lösungen, 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 (Serviceprodukte) sowie zuverlässiges Facility- und Applikationsmanagement. Dies wird transparent durch:
 - Facility Management (z. B. reibungsloser Betrieb der Rechenzentren)
 - Erreichbarkeit und schnelles Reagieren im Emergency-Fall
 - Datensicherheit und Datenschutz
 - Zuverlässige System-Technik
 - Schneller und kompetenter Kundensupport
 - Professionelles Training für Kunden
- Durchführung von erfolgreichen und zufriedenstellenden, professionellen Projekten (Kundenprojekte und interne Projekte). Dies wird transparent durch:
 - Professionelles Projektmanagement
 - 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
- Eine 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.

2.1.3 Qualitätspolitik

Die Qualitätspolitik der AEB basiert auf dem Unternehmenshandbuch (AEB Guideline).

Im Wesentlichen sieht sich das QM dabei in der folgenden Verantwortung bzw. verfolgt stets das Ziel unseren wertschöpfenden Geschäftsbetrieb bzw. -prozess sicherzustellen.

Das heißt, unsere Service- und Cloud-Angebots-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 Rollen 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 Mitarbeiter im Rahmen ihrer Arbeit bzw. ihrer Rolle bei 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

Sicherheitsziele sind Sicherheitsvorgaben mit Korridoren, die messbare und überwachbare Größen darstellen.

Sicherheitsziele machen somit den Erhalt von Sicherheit kontrollierbar und Risiken bewertbar.

Sicherheitsziele werden als KPI in der Liste Sicherheitsziele KPI geführt, gepflegt und ihre Einhaltung regelmäßig einem Monitoring unterworfen.

Die Überwachung der Sicherheitsziele erfolgt mindestens im Rahmen der ISMS-Managementbewertungen.

Unsere maßgeblichen **Schutzziele** sind Verfügbarkeit, Vertraulichkeit und Integrität.

- 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 gestaltet.

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 externe 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.)

2.2.1 Sicherheit – die wichtigsten Regeln

Die AEB legt sich mit dem 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 Mitarbeiter 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

2.3 Leitsätze zum Datenschutz

Als relevante Norm sehen wir die europäische Datenschutz-Grundverordnung (kurz: DS-GVO) samt relevanter anwendbarer nationaler Datenschutzgesetze.

Wir bekennen uns zu den Datenschutz-Prinzipien (wie in ISO 29100 formuliert) mit dem Hauptziel „Schutz der Betroffenen“, sowie zur Erfüllung der Pflichten gegenüber Verantwortlichen im Verhältnis der datenschutzrechtlichen Auftragsverarbeitung gemäß Art. 28 DS-GVO.

Bestandteil ist eine Risikobetrachtung aus Sicht der Betroffenen gemäß Art. 4 DS-GVO mit einer Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO.

Näheres führen wir separat in unserer Datenschutzleitlinie aus, die ebenfalls im AEB Trust Center verfügbar ist.

Das Sicherheitskonzept der AEB integriert Sicherheitsmaßnahmen aus den Perspektiven:

- Informationssicherheit (mit den SoA der ISO 27001, den Controls der Erklärung zur Anwendbarkeit)
- Datenschutz (mit den ergänzenden Maßnahmen der ISO 27018 sowie den Anforderungen und Pflichten gemäß Art. 32 DS-GVO)

3 Organisationsstrukturen im IMS

3.1 Rollen, Verantwortlichkeiten und Ressourcen

3.1.1 Einführung

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

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.

3.1.2 Rollen im Security- und Datenschutzkontext

Die relevanten Rollen sind:

Rolle	Funktion, Verantwortung	Mitglied in	Kommentar
Geschäftsführung (Verwaltungsrat)	<ul style="list-style-type: none"> • 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 	AEB Security Sync, ISMS Report, BCM Report, DS Report	Höchste Instanz der Verantwortung
ISMS Manager	<ul style="list-style-type: none"> • Verantwortlicher für den Betrieb des Managementsystems ISMS • Betrieb des PDCA-Zyklus zum Betrieb des ISMS 	IS-Board, ISMS Report	

Rolle	Funktion, Verantwortung	Mitglied in	Kommentar
	<ul style="list-style-type: none"> • Leitung des IS-Boards • Controlling des ISMS gemäß unseren Vorgaben, insbesondere auch der Einhaltung regelmäßiger Aktivitäten • Veranlassung interner Audits • Erklärung der Anwendbarkeit erstellen • Dokumentation von Management-Änderungen • Sicherstellung Dokumentenlenkung • Wahrung der Kontakte zu Behörden und zu sicherheitsrelevanten Interessengruppen 		
IT Security Manager	<ul style="list-style-type: none"> • 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 	AEB Security Sync, Security Operativ, SSA, IS-Board, ISMS Report, DS Report	
ISMS-Leitung (Sicherheits-Management)	<ul style="list-style-type: none"> • 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 Rollen ISMS Manager und IT Security Manager zusammen
Domänen-Sicherheitsbeauftragte	<ul style="list-style-type: none"> • Die Domänensicherheitsbeauftragten sind für die Durchsetzung der relevanten Sicherheitsvorgaben in ihrer Domäne verantwortlich. 	IS-Board	

Rolle	Funktion, Verantwortung	Mitglied in	Kommentar
	<ul style="list-style-type: none"> 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. Sie sind entsprechend u. a. für den Betrieb des ISMS geschult und eingearbeitet. 		
Security Verantwortliche	<ul style="list-style-type: none"> Das Funktionieren der Security Organisation und das Reagieren auf Security Vorfälle 	Security Operativ	
Datenschutzbeauftragter (DSB)	<ul style="list-style-type: none"> Hinwirken auf die Einhaltung der DSGVO und des BDSG Wahrung der Kontakte zu Behörden und zu sicherheitsrelevanten Interessengruppen 	DS Report, AEB Security Sync, Security Operativ	
Mitarbeiter im Datenschutzbetrieb	<ul style="list-style-type: none"> Arbeiten auf die Einhaltung der datenschutzrechtlichen Verpflichtungen im Unternehmen hin Aktive Unterstützung des Datenschutzbeauftragten 	DS Report, Security Operativ	
Compliance Officer	<ul style="list-style-type: none"> Rechtskonformität Monitoring auch von Änderungen von relevanten gesetzlichen Vorgaben 	IS-Board	gemäß A.18
Notfallbeauftragter	<ul style="list-style-type: none"> Der Notfallbeauftragte steuert alle Aktivitäten rund um die Notfallvorsorge und wirkt bei den damit verbundenen Aufgaben mit. Er ist für die Erstellung, Umsetzung, Pflege und Betreuung des Notfallmanagements sowie der zugehörigen Dokumente und Regelungen in allen Phasen unternehmensweit zuständig. 	BCM Report IS-Board BCM Sync	

3.1.3 Domänen-Sicherheitsbeauftragte, Eigentümer und Verantwortung

- Für nachfolgend gelistete Domänen, die in direktem Zusammenhang mit unseren Hauptgeschäftsprozessen 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 und Compliance mit Themen zu <ul style="list-style-type: none"> • Recht und Gesetz, Compliance, Datenschutz • Kaufm. Abwicklung, Controlling, Buchhaltung
2	Mitarbeiterbetreuung (Personal/HR)
3	Infrastruktur mit Themen zu <ul style="list-style-type: none"> • Haustechnik • Team Care
4	IT mit Themen zu <ul style="list-style-type: none"> • Systemmanagement • Rechenzentrum
5	Services mit Themen zu <ul style="list-style-type: none"> • Support
6	Produkte / Standard-Softwareentwicklung
7	Lösungen (Kundenprojekte)
8	Vertrieb/Vermarktung

Die genauere Zuständigkeit wird im IS-Board im Abschnitt Regelungsbereiche verdeutlicht.

3.1.4 QM Verantwortung

Das QM wird vor allem durch die Mitarbeiter selbst im Rahmen ihrer Rolle 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 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, Verfahren und Qualitätssichernde Maßnahmen, Tools, Schulungen etc. festlegen wollen. Durch regelmäßigen Austausch 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 im unternehmenseigenen Confluence 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 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	E-Mail (und Meeting); Dokumentation in Korrektur- und Vorbeugemaßnahmen
Änderung der Organisation	Inhalte der Änderung, Gründe	Leiter der Organisation	QMS Verantwortliche, betroffene Mitarbeiter	E-Mail, Intranet-Nachrichten, bei Bedarf Nachschulung
Änderung an Guides	Inhalte der Änderung, Gründe	Verantwortlicher des Guides	Belegschaft oder betroffen Domäne, entsprechende Zielgruppe	Intranet-Nachrichten, bei Bedarf Nachschulung

Im firmeninternen Intranet (WIKI) werden Informationen transparent zur Verfügung gestellt. Intranet-Nachrichten nehmen häufig zu weiteren Ausführungen Bezug auf WIKI.

3.5 Dokumentierte Informationen

3.5.1 Allgemeines

Die Organisation hat zur Beachtung genereller Dokumentationsanforderungen eine Richtlinie zur Dokumentation erstellt.

Siehe Dokumentenlenkung (QMS).

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 großgeschrieben. Pflichtschulungen gehören zum Onboarding und müssen von jedem neuen Mitarbeiter besucht werden. Als Pflichtschulungen eingestuft sind z. B. aufgrund ihres hohen Stellenwerts Schulungen zur Sicherheit (Arbeitsschutz, Datenschutz, Datensicherheit, ISMS). Nähere Informationen findet man in Confluence in dem Bereich Wissensmanagement, dort unter: Pyramide Sicherheit

- Die Audits – auch die internen – werden protokolliert.

3.5.2 Weitere regelmäßige Aktivitäten

im QMS

- Aktualisierung aller Regeln und Prinzipien (1x / Jahr)
- Aktualisierung der Wertschöpfungskette und aller hinterlegten Prozesse inkl. Rollen (1x / Jahr)
- Internes 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

im DSMS

- Wiederholung der Datenschutz-Folgenabschätzung; mindestens 1 x / Jahr
- Regelmäßige Kontrollen (z.B. zu Dokumenten, Verzeichnissen, Konformität bei Datenübermittlungen in Drittland mit Durchführung TIA, dem Transfer Impact Assessment)
- Mit ISMS koordiniertes Releasemanagement zum Sicherheitskonzept; ca. 1 x / Jahr
- Regelmäßiges Reporting; mindestens 1 x / Jahr

4 PDCA im IMS

4.1 Führung

4.1.1 Führung und Engagement

Aus dem Selbstverständnis der AEB wie wir agieren wollen und wie wir auf dem Markt auftreten leitet sich unser hoher Anspruch an Qualität, Datenschutz und Sicherheit ab. Die Geschäftsführung legt hierauf besonderen Wert und versteht sich in der Verantwortung für Qualitätsmanagement, Datenschutz 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, Datenschutz 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-, Datenschutz- 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.

4.1.2 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.

4.1.3 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.

4.2.1 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 [ISMS Guide](#).

4.2.2 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.

4.2.3 Betrachtungen im Umfeld des DSMS

Im Umfeld des Datenschutzes ist eine besondere Betrachtung aus Sicht der Betroffenen erforderlich. Die Mechanismen des ISMS wurden dazu weitgehend auf das Schutzziel der Betroffenen adaptiert; sowohl für eigene Mitarbeiter als auch Personen u.a. in den Systemen, die der datenschutzrechtlichen Auftragsverarbeitung unterliegen. Ergebnisse dazu bringen wir regelmäßig in der Prüfung zur Datenschutz-Folgenabschätzung zum Ausdruck. Eine Regelung zum Umgang mit Datenpannen ist etabliert.

4.3 Planung von Veränderungen

Durch regelmäßige interne Audits überprüfen wir sowohl das QMS, das DSMS 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:

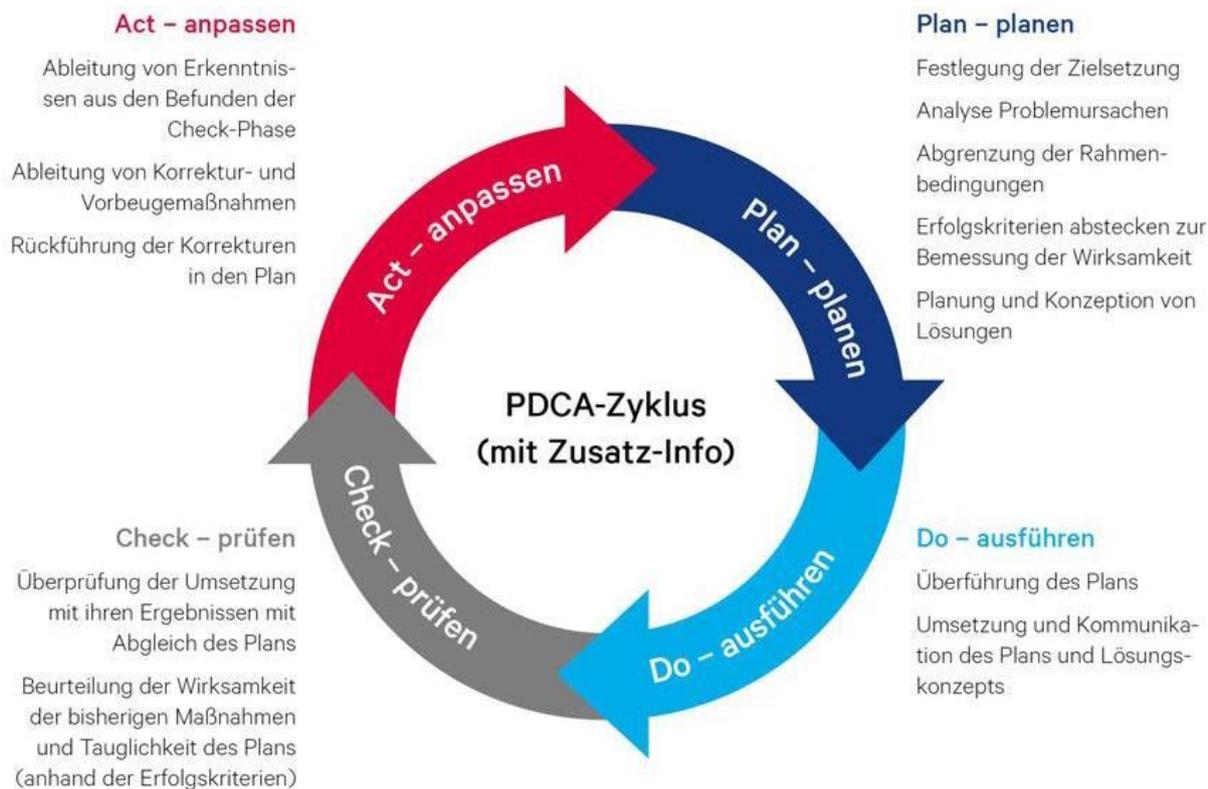
4.3.1 Zertifikate

Auf der Wiki Seite [Zertifikate \[DE\]](#) sind alle Zertifikate der AEB zu finden. Auf der AEB Webseite sind im [Trust Center](#) alle Zertifikate zu finden, wie wir sie auch extern bereitstellen.

4.3.2 QM-gesteuerte Veränderungen

Die Managementsysteme orientieren sich im Rahmen ihrer 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, Datenschutz oder Sicherheit)
- und steht für: "Plan-, Do-, Check-, Act-Zyklus" Dieses Prinzip verwenden wir daher in
- unserem Qualitätsmanagement (QMS)
- unserem Informationssicherheitsmanagement (ISMS)



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 Tickets an Recht oder 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 Wissensmanagements 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 und 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 bekanntgegeben und zur Diskussion gestellt.

- Mehr Details zum Wissensmanagement findet sich im Bereich [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

4.5.1 ISMS

- Zur Umsetzung dieser Leitlinie für die Informationssicherheit steht ein [ISMS Guide](#) zur Verfügung. Dieser regelt u. a. die regelmäßige
 - Risikoeinschätzung
 - Risikobehandlung

4.5.2 QMS

- Die Umsetzung des QMS wird auf der AEB-internen Seite [Qualitätsmanagement \[DE\]](#) ausführlich erläutert.
- Für einen kurzen Auszug auch zu Durchsetzungsmaßnahmen siehe Abschnitt Qualitätspolitik.

4.5.3 DSMS

- Die Umsetzung des DSMS und ihre Pflege wird auf der AEB-internen Seite [Datenschutzmanagementsystem](#) ausführlich erläutert.
- Die Datenschutzleitlinie steht im AEB Trust Center (Einstieg Datenschutz) zur Verfügung.

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, Datenschutzbeauftragter	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

Instrument	Beteiligte Rollen	Indikatoren und Messlatte in der Wirksamkeitsprüfung
Kunden-Befragungen, Feedback einholen	Marketing, Service-Organisation	Auftreten des Risikos zum Ausdruck bringen. Beispiel: Anzahl Tickets mit def. Symptom. Aktion-getriebene Fragebögen; Auswertung

4.7 Verbesserung

Die letzte Phase Verbesserung schließt den Kreislauf zum geregelten iterativen Prozess, in dem 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

4.7.1 Weitere wesentliche Dokumente

- [Security Guide](#)
- [ISMS Guide](#)
- [QM Guideline](#)
- [Datenschutzleitlinie](#)