Guideline

Integrated Management System (IMS)

August 30, 2024

www.aeb.com

Contents

1	**Guideline and rules for information security, data protection and quality policy**	**1**
1.1	Purpose and basic claim	2
1.2	Specifications and requirements	2
1.2.1	Business requirements	3
1.2.2	Legal requirements	4
1.2.3	Contractual requirements	4
1.2.4	Other regulatory requirements	5
1.3	Application areas	5
1.3.1	On ISO 9001 – procedures and processes	5
1.3.2	Reason for the selection	5
1.3.3	On ISO 27001 – procedures and processes	5
1.3.4	Reason for the selection	6
1.3.5	On ISO 27018 – procedures and processes	6
1.3.6	Reason for the selection	6
2	**The QMS, DPMS, and ISMS management systems in the IMS**	**6**
2.1	Basic principles of quality policy	7
2.1.1	AEB quality standard	7
2.1.2	Detailed quality objectives	7
2.1.3	Quality policy	9
2.2	Basic principles of the security strategy	9
2.2.1	Security – the most important rules	11
2.3	Guiding principles on data protection	11
3	**IMS organizational structures**	**12**
3.1	Roles, responsibilities, and resources	12

3.1.1	Introduction	12
3.1.2	Roles in the security and data protection context	12
3.1.3	Domain Security Officers, owners, and responsibility	14
3.1.4	Responsibility for QM	15
3.2	Administration	16
3.3	Competences and awareness	16
3.4	Communication	17
3.5	Documented information	17
3.5.1	General	17
3.5.2	Further regular activities	18
4	**PDCA in the IMS**	**18**
4.1	Leadership	18
4.1.1	Leadership and commitment	18
4.1.2	Guidelines on management systems	19
4.1.3	Organizational tasks, responsibilities, and authorizations	19
4.2	Dealing with opportunities and risks	19
4.2.1	Considerations in the ISMS environment	19
4.2.2	Considerations in the QMS environment	19
4.2.3	Considerations in the DPMS environment	20
4.3	Planning for changes	20
4.3.1	Certificates	20
4.3.2	Changes controlled by QM	20
4.4	Meaning of the knowledge management for the IMS	21
4.5	Operations / use	22
4.5.1	ISMS	22
4.5.2	QMS	22
4.5.3	DPMS	22
4.6	Ensuring control and effectiveness	22

4.7 Improvement 24

4.7.1 Further important documents 24

Note: In this documentation there are some links that allow AEB employees to open further information on the AEB intranet. This illustrates the high degree of integration of AEB's knowledge management.

1 Guideline and rules for information security, data protection and quality policy

This document is a comprehensive AEB guideline describing AEB's quality standards. The integrated Information Security Guideline is directed at all parties concerned with information security and regulates security management.

The content of the guideline is oriented at the new high level structure of the ISO 9001, ISO 27018, and ISO 27001 standards.

This guideline covers the following chapters:

Chapter in ISO standard	Content, purpose	To be found in section
4 – Environment of the organization	• Perception of the organization • Interested parties and their expectations • Application areas of quality management system or information security management system	• Section 1.2 • Section 1.2 • Section 1.3
5 – Leadership (behavior)	• Leadership and self-commitment • Quality policy • Tasks, responsibilities, authorizations	• Sect. 1.1, Sect. 4.1.1 • Section 2.1 • Section 4.1.3
6 - Planning	• (Dealing with) opportunities and risks • Quality objectives • Planning for changes	• Section 4.2 • Section 2.1 • Section 4.3
7 - Support	• Resources • Competency • Awareness • Communication • Documented information	• Sect. 3.1, Sect. 3.2 • Section 3.3 • Section 3.3 • Section 3.4 • Section 3.5

The above-mentioned ISO standard chapters 4-7 comprise the planning phase of the process-oriented PDCA cycle. Structure-wise, we have decided to organize chapters differently at AEB.

- Chapter 1 deals with the overall objectives and requirements, with AEB's self-perception regarding security, quality, and data protection
- Chapter 2 follows with statements on the application areas of management systems
- Chapter 3 is dedicated to the organization in which 'people' are the focus and undertake tasks with responsibilities in their roles
- Chapter 4 addresses the process-oriented PDCA approach and also makes statements on the remaining chapters 8-10 of the ISO standard

The chapters are allocated to the other phases of the PDCA cycle in the following way:

Chapter in ISO standard	Function, content	PDCA phase	To be found in section
8 - Operations	Operations / use	Do	Section 4.5
9 - Performance assessment	Performance assessment (ensuring control and effectiveness)	Check	Section 4.6
10 - Improvement	Improvement	Act	Section 4.7

We are trying to present the general statements on the management systems for quality, data protection, and security here. For specific statements on quality, data protection, or security, please refer to the separate sections for better readability.

1.1 Purpose and basic claim

This guideline is to be kept relatively stable. It is part of company culture and expresses a declaration of intent by top management. It includes generic policy statements on quality, data security, and information security (framework for defining objectives, principles of action, etc.) For orientation, we rely heavily on ISO 9001, ISO 27018, and ISO 27001. We have been certified for the ISO 27001 standard since February 2010.

- Rules keep changing; we live in a dynamic world.
- First and foremost, quality, data protection, and security mean awareness.
- Quality, data protection, and security are a claim whose realization has to be trained. Therefore, we see the management of these topics as a commitment, a general attitude, and a process of continuous improvement. We are oriented towards long-term relationships.

1.2 Specifications and requirements

Objective: Which specifications of which interested parties describe the context of the organization and thus influence conformity?

In an overview:

Party	Interests	Interfaces	Controlled through
Customers	Fulfillment of contractual obligations; product expectations according to current market demands based on state-of-the-art technology; legal compliance etc.; expectations regarding business continuity	General Terms & Conditions: contractual commitment (license, support, SLA, NDA); statements in system descriptions	Product management, legal, service organization (e.g. SLA management) Maintenance and control of security measures
Legislature	Compliance	Transfer through training, for example	Legal team; data protection officer, central contract management; compliance officer
Service provider	Remuneration	(Service) contracts	Partner manager; comprehensive partner management with control function
Partner	Remuneration; support of the partnership to reach common goals, including strategic orientation	(Partner) contracts	Partner manager; controls; regular exchange
End user	Usability, performance of the applications; hotline availability	System descriptions, online help, support	Product management, marketing, feedback from seminars, for example; support organization
Customs authority	Communication according to certified procedures	Certified procedures	Product Management
Insurances	Compliance with contractual conditions	Contracts including insurance	Regular exchange and review
Employees	Health environment; good atmosphere; ethical correctness	Occupational safety; consensual culture	Ongoing exchange; awareness, code of conduct; guidelines

Further explanations:

1.2.1 Business requirements

Our customers are in the focus of our quality claim and their trust and satisfaction with AEB solutions supporting their business processes are the measure of success.

Our cloud solutions also require us to fulfill security, data protection, and quality demands resulting from legal requirements for our customers and their processes. AEB ensures a high degree of compliance of data protection and security standards due to its role and activities as service provider in the context of its industry environment. Internationalization necessitates orientation according to internationally recognized standards.

The quality standard is immediately derived from the conditions and requirements for using the products and services.

AEB deems the data protection and security perspectives an increasingly critical decision criterion in the market. These perspectives mean more than just mastering the technical facets. They include organizational structures and compliance with legal requirements, especially in the field of the products and services that our customers use in their day-to-day business processes.

Climate change is a relevant topic for AEB. AEB has integrated this aspect into the risk assessment of our ISO-certified ISMS. Threats of force majeure (such as storms, floods, extreme heat) are the subject of regular observation and assessment.

We see it as an opportunity to make a contribution based on our own ethical standards and sense of responsibility, both to make our own contribution to curbing climate change and to demonstrate our resilience to the effects of climate change, thereby protecting our customer services and making a conscientious commitment.

1.2.2 Legal requirements

The list of relevant laws and regulations is regularly reviewed for relevance. This includes in particular:

- KonTraG (requirement to implement a monitoring system; early detection; statements on risk structure; proof of traceability on functioning of a control system)
- GDPdU, GoBD, GoBS (due diligence obligations for processing, retaining, and providing information, particularly invoice-relevant data for accounting and tax audits; request to set up an internal control system)
- GDPR, BDSG (data protection, provision of a security concept in accordance with Art. 32 GDPR – technical and organizational measures; care with regard to the personal rights of those affected, data economy, confidentiality, appropriateness to a specific purpose, etc.)
- TKG, DDG, TDDDG (telecommunications and telemedia)
- IT Security Act (NIS Directive, KRITIS, with significance for critical infrastructures)
- Basel III (indirectly via requirements to banks as lenders)
- Relevant laws and (industry) requirements in foreign trade: AEB's applications are based in a sensitive, very dynamic, and international environment in which country-specific and international politics exert influence on what is currently perceived as correct and compliant. Some keywords include: export restrictions, war weapons according to the German War Weapons Control Act (WWCA), armaments according to the Foreign Trade and Payments Ordinance (AWV), dual-use, embargo lists. This means that authorities such as the Federal Office for Economic Affairs and Export Control (BAFA) are also important sources.

1.2.3 Contractual requirements

- In Service Level Agreements (SLA) with the customer, we agree on quantified quality goals and their fulfillment (e.g. response times, availabilities).
- The GDPR specifies requirements on special duty of care when dealing with customers, partners, and subcontractors (see data processing as defined by Art. 28 GDPR). A data protection officer has been appointed.

- Conclusion of nondisclosure agreements (NDA) with business partners (customers, partners, subcontractors); internally, employees are bound to data secrecy and are made aware and trained in the confidential handling of information.
- NDAs are concluded with subcontractors. If subcontractors have access to the system (for example, for maintaining applications), separate system access contracts are concluded, which limit access to the necessary minimum.

1.2.4 Other regulatory requirements

All employees of the organization are asked and obliged to comply with the above-mentioned requirements. Generally, every employee is responsible to contribute actively to quality assurance. The awareness, vigilance, and realization of measures assuring quality as well as trainings, such as emergency management

- are trained as part of AEB's mandatory trainings,
- continuously monitored in meetings of those responsible,
- and are checked regularly during internal audits.

To ensure sustainability (effectiveness of ISMS, DPMS, and QMS)

- a PDCA cycle has been defined which also include responsibilities and rules (see below)
- all employees are asked to turn to the respective responsible person if changes occur in the environment, which will affect security-related aspects
- the specifications of the ISO 9001, ISO 27018, and ISO 27001 standards and the corresponding management systems provide orientation

1.3 Application areas

1.3.1 On ISO 9001 – procedures and processes

The application area refers to the whole company and therefore includes:

- all locations
- all products

1.3.2 Reason for the selection

With the importance of cloud offerings and services for the value-added processes of companies (AEB customers), their demand for the quality of AEB's offer is a central focus point. For AEB, it is important to convince customers with standard cloud offerings, individual solutions, and services which will satisfy their expectations in the long-term and meet the highest quality standards.

1.3.3 On ISO 27001 – procedures and processes

The application area comprises the AEB customer data centers in Stuttgart as well as software development.

- Location: Stuttgart, Sigmaringer Strasse 109
- System: Operation of the hosted systems as well as further services for our customers; applies to all AEB applications
- Interfaces: These are access systems for remote access (Citrix server, WebServer for Internet connections,...), connections with customs, for example.
- Values: Values and risks are listed in detail in the risk management tool provided for this. Adjacent processes are the following
    - Service/support: Change management process
    - Customer projects: Release management process
    - Facility management for customer data centers
    - Additional services by partners: Partner management process, for access with partner contracts for system access

1.3.4 Reason for the selection

- Focus on core functionality
- High protection need for operating the data center
- The customer data centers and product development account for a significant share of our business

1.3.5 On ISO 27018 – procedures and processes

The application area refers to the whole company and therefore includes:

- all persons
- all locations
- all products
- all customers

1.3.6 Reason for the selection

- A restriction of the scope is neither intended nor useful here

2 The QMS, DPMS, and ISMS management systems in the IMS

Process-oriented management systems ensure operation and continuous improvement. This includes, amongst other things,

- a guideline with clarification of objectives and organization
- tools for monitoring of effectiveness

- administrative tools and process-oriented working for operation, monitoring, and improvement
- risk management

The objectives of the management systems are to be communicated regularly and have to be updated if necessary.

2.1 Basic principles of quality policy

2.1.1 AEB quality standard

The desired quality level for AEB and our own quality standard resulting from general customer requirements and expectations is specified by the Board of Directors as follows:

AEB's quality standard aims at...

- introducing solutions that satisfy our customers' requirements and delight them.
- developing integrated cloud offerings (standard software products) with a high usability fulfilling the needs of the market at reasonable prices and operate reliably.
- providing integrated, reliable services (service products), accessibility, and quick response in emergency situations, and a reliable facility management (e.g. smooth operation of the data center). While doing so, we handle customer data and wishes securely and confidentially.
- carrying out successful and satisfactory projects (customer projects and internal projects) in a professional and economical way. Always aware that something unexpected may arise, necessitating a flexible response. We also ensure that roles and tasks are clearly distributed both at AEB and on the side of the customer allow both sides to engage in a sincere and professional cooperation.
- pursuing successful, sustainable marketing of our products and the company.
- This includes reliable, competent, and transparent communication with the market and our partners. Reliability and requirements traceability from quotation to order.
- running an efficient and transparent administration that ensures compliance with legal regulations and contracts. Streamlined processes in commercial transactions closely interwoven with other areas.
- providing transparent and reliable employee services which promote every individual's wellbeing and work at the company.
- Ensuring high quality levels of training and continuing education to keep internal knowledge and competences at a high level.

2.1.2 Detailed quality objectives

- Successful and sustainable marketing of the cloud offerings and the company. This is made transparent by:
    - Reliable, competent, and transparent communication with the market and our partners.
    - Reliability and requirements traceability from proposal to order
    - Sales and marketing processes guided by high service quality

    - Secure and confidential handling of customer data
- Development of integrated cloud offerings with a high usability fulfilling the needs of the market at reasonable prices and operating reliably. This is made transparent by:
    - Fulfillment of technical requirements (competitive software solutions) and being up to date (regular updates)
    - Self-explanatory and fit for use cloud offerings (friendly, ergonomic, intuitive, tangible, and easy to use)
    - Striving for accuracy (every line of code is approved and tested)
    - Securing maintainability and smooth operation
- Introduction of solutions that meet our customers' requirements. This is made transparent by:
    - Integrated solutions (mix of software and services)
    - Adaptations tailored to the specific needs of customers and the industry that can be maintained efficiently and transparently.
- Consistent and comprehensive services (service products) as well as reliable facility and application management. This is made transparent by:
    - Facility Management (e.g. smooth data center operation)
    - Availability and quick response in case of emergency
    - Data security and data protection
    - Reliable system technology
    - Quick and competent customer support
    - Professional training for customers
- Implementation of successful and satisfying professional projects (customer projects and internal projects) This is made transparent by:
    - Professional project management
    - Realizing economically viable projects
    - Clear distribution of roles and tasks on either side
    - Being aware of unforeseen events and able to respond flexibly to these events
    - Open and competent cooperation
- running an efficient and transparent administration that ensures compliance with legal regulations and contracts. This is made transparent by:
    - Compliance with the law, with regulations and with contracts
    - Streamlined processes in commercial transactions closely interwoven with other areas
    - Comprehensibility and efficiency in communication and contracts
    - Fast response time regarding inquiries and complaints
    - Ensuring high quality levels of training and continuing education to keep internal knowledge and competence at a high level.

2.1.3 Quality policy

AEB's quality policy is based on the company manual (AEB Guideline).

In essence, QM is responsible for the following and always pursues the goal of ensuring our value-added business operations and processes.

Our value creation from services and cloud offerings must run smoothly. Otherwise, our company's success would be at risk. QM and QMS of AEB are tailored to the employees and their capabilities and roles in everyday working life. As a result, they are permanently embraced and implemented. Both is based on an integrated roles concept which promotes and strengthens the personal responsibility of every employee to create value within the corporate context.

QM is practiced as part of each employee's roles – within the framework provided by the QMS.

AEB's underlying principles are the following:

- Professionals assume responsibility for (the quality of) their work on a daily basis in a conscientious manner.
- As part of their work or role(s) at AEB, all employees are responsible to achieve the desired quality and practice quality management.
- The corresponding roles define processes, requirements, and tools and are responsible that they always remain up to date and meaningful.
- A centralized, synchronized, and managed QMS created the necessary framework for this, provides the corresponding tools to create synergies and integration – but does not take any content-related decisions and avoids compensating the responsibility of the employees.

The goal is to map as much as necessary but as little as possible in the form of transparent and fit for purpose standards (rules & principles). The result should be a healthy balance between regulations and responsibility to preserve the flexibility necessary to be able to react appropriately and competently to special requirements.

We therefore distinguish between generally valid rules (topics), specific (primary and secondary) core processes without which our value creation cannot be effective and accompanying processes that contribute to efficient workflows (e.g. within teams, in cooperation with other teams).

2.2 Basic principles of the security strategy

Security objectives are security requirements with corridors that are measurable and monitorable quantities.

Security objectives thus make the maintenance of security controllable and risks assessable.

Security objectives are maintained as KPIs in the Security Objectives KPIs list, and their compliance is regularly monitored.

Security objectives are at least monitored as part of ISMS management assessments.

Our most important protection objectives are availability, confidentiality, and integrity.

- Availability does not only refer to technical aspects of accessibility of our IT solutions, but also to organizational availability of contacts for customer support, for example. Related agreements are part of the General Terms & Conditions, standard contracts or separate individual agreements.

- Confidentiality does not only relate to technical aspects such as access restrictions according to assignments, but also to the clarification of and binding agreement on authorizations for our employees when handling data, particularly of our business partners.
- Integrity calls for clear processes in information processing in particular.

Modeled after COSO, an internal control system (ICS) has been set up to secure basic strategies and principles, such as the following:

- Request for separation of functions
- Verification of critical activities by a second user (release of patches, guides, contracts, assignment of user rights,...)
- Transparency principle (documentation obligation)
- Rules on confidentiality (e.g. need-to-know principle)
- Using risk management (ISMS)

Our security strategy is based on the principle of individually protecting applications, data, networks, devices, and users. We ensure this through state-of-the-art technology and a structured process-controlled approach.

For the risk analysis process, we want to follow the model mix of "security from the inside to the outside" or "security by ownership". Generally, every detected (significant) information is an asset worth protecting. We therefore follow an analytical approach with the following characteristics:

- Cataloging the information in the application area (including related areas)
- Clear assignment of persons responsible for the information
- Risk assessment and protection measures are developed as close to the information as possible and aligned with the specifications of this policy
- If the need for protection of the information can be met effectively through measures at a higher modeling level, these have priority
- For this reason, the cataloging has to be modeled in a way that allows for the adequate operation of the ISMS with security measures.

The ISMS helps to achieve greater security of action. This will also make the process of dealing with risks more efficient.

The ISMS should be suitable to achieve the security objectives and should be the basis for a binding value system from the security perspective.

The ratio of effort and risk reduction should be appropriate to the protection needs of the application area. A strategic risk management has been put in place, which aligns measures with guidelines and keeps them compliant.

The ISMS should be flexible enough to adapt to changing conditions or objectives. Continuous operation creates sustainability.

The ISMS is also a tool for prevention and problem avoidance. Our activities in this regard include:

- Various regular checks, and internal and external audits. To test our security, we simulate internal and external attacks regularly. We commission external service providers to carry out these penetration tests.
- Early detection principle (monitoring and alerting of the systems)
- Thorough follow-ups, analysis of causes (e.g. when emergencies have occurred)

- Operation of an emergency concept and an emergency organization
- Performance of emergency drills (based on simulated scenarios)
- Continuous security awareness activities (campaigns, training, news, etc.)

2.2.1 Security – the most important rules

The Security Guide imposes binding rules on AEB, which are observed and supported by the employees. Here's an excerpt of the most important rules:

- Security is every employee's business; security incidents are administered through a central tool
- Clean desk rules; workplace security (virus protection, etc.)
- Ensuring duty of care with confidentiality statements
- Working with accounts and passwords
- Handling data outside the company or outside the EU/EEC
- Dealing with guests
- Observing data protection (internally and externally)
- Regular participation in trainings (on security awareness)
- Ensuring that nondisclosure agreements are concluded with business partners if necessary

2.3 Guiding principles on data protection

We consider the relevant standard to be the European General Data Protection Regulation (in short: GDPR) together with relevant applicable national data protection laws.

We are committed to the data protection principles (as formulated in ISO 29100) with the main objective "protection of data subjects", as well as to the fulfillment of obligations towards data controllers in regards to commissioned processing of data under data protection law in accordance with Article 28 GDPR.

Part of this is a risk assessment from the perspective of the data subjects pursuant to Article 4 of the GDPR with a data protection impact assessment pursuant to Article 35 of the GDPR.

We provide more details separately in our data protection guideline, which is also available in the AEB Trust Center.

AEB's security concept integrates security measures from the perspectives:

- Information security (with the SoA of ISO 27001, the controls of the statement of applicability)
- Data protection (with the supplementary measures of ISO 27018 as well as the requirements and obligations according to Article 32 GDPR)

3 IMS organizational structures

3.1 Roles, responsibilities, and resources

3.1.1 Introduction

The approval of the management on the IMS guideline also signifies their general approval of the identified risks that will be accepted.

AEB uses a distinctive roles concept. The current instances and the owners of roles can be taken from the organizational structure according to the valid organizational documentation.

A role description includes the responsibility, tasks, and competences as well as requirements, relevant processes, and permissions. The permission concept is linked to the roles. Employees can find information on their roles via a standardized tool.

3.1.2 Roles in the security and data protection context

The relevant roles are:

Role	Capacity, responsibility	Member in	Notes
Management Board (Board of Directors)	• Instructing functions, main responsibility for effectiveness of management systems • Approving these guidelines • Approving organization for QMS and ISMS • Managing evaluation and review • Promoting continuous improvement • Approving resources and means • Taking decisions on risk acceptance criteria	AEB Security Sync, ISMS report BCM report DS report	Highest responsible body
ISMS Manager	• Responsible for the operation of the ISMS management system • Operating the PDCA cycle for operating ISMS • Management of the IS Board • Controlling the ISMS according to our specifications, particularly if regular activities are observed • Initiating internal audits • Creating an explanation of the applicability • Documenting management changes • Ensuring document guidance	IS Board ISMS report	

Role	Capacity, responsibility	Member in	Notes
	• Preserving contacts with authorities and security-relevant interest groups		
IT Security Manager	• Avoidance of risks to the entire company. • Coordination of roles and processes relevant for security. • Main responsibility for the Security Guide. • Defines company-wide information security standards. • Ensures the implementation of and compliance with security standards. • Coordinates security analysis. • Preserving contacts with authorities and security-relevant interest groups	AEB Security Sync, Security Operativ, SSA, IS Board ISMS report DS report	
ISMS management (security management)	• Monitoring work on the risk treatment plan • Evaluating the effectiveness of measures • Reporting security incidents • Offering modules on security training and ISMS awareness • Initiating and monitoring security checks	IS Board	The ISMS management consists of the role owners of the ISMS management and IT Security Manager roles.
Domain Security Officer	• The Domain Security Officers are responsible for enforcing the relevant security specifications in their domains. • They are also responsible for carrying out the risk observation, including risk treatment. • If necessary, they include the respective asset owners in this process. • Accordingly, they have been trained to operate the ISMS, among others.	IS Board	
Security Officers	• The functioning of the security organization and the reaction to security incidents	Security Operativ	
Data protection officer	• Working towards compliance with the GDPR and the BDSG (German Federal Data Protection Act) • Preserving contacts with authorities and security-relevant interest groups	DS report AEB Security Sync, Security Operativ	
Employees in data protection	• They work towards compliance with data protection obligations in the company	DS report	

Role	Capacity, responsibility	Member in	Notes
	• Active support of the Data Protection Officer	Security Operativ	
Compliance Officer	• Legal compliance • Monitoring changes of relevant legal regulations	IS Board	according to A.18
Emergency Officer	• The Emergency Officer controls all activities of emergency planning and contribute to related tasks. The Emergency Officer is responsible for creating, implementing, maintaining, and supporting all phases of the company-wide emergency management as well as related documents and regulations.	BCM report IS Board BCM sync	

3.1.3 Domain Security Officers, owners, and responsibility

- For each of the domains listed below, which are connected directly to our core business processes, the role of '"Domain Security Officer"' was established. Each Domain Security Officer was assigned to be responsible for one or several of the "regulatory areas" of the ISO standard.
- In their domain, the Domain Security Officers are responsible for performing the risk observation. For this, they involve the asset owners in the process.
- Details and detail assignments are defined in an internal documentation. There, a responsible person is assigned for each control objective. The Domain Security Officers regularly check the documentation relevant for their field of action for their responsibility and the realization of the measure objective.

No.	Domain
1	Administration and Compliance with topics on • Law, compliance, data protection • Commercial Processing, Controlling, Accounting
2	Employee Services (Personnel/HR)
3	Infrastructure with topics regarding • Building services • Team Care
4	IT with topics regarding • System management • Data center
5	Services with topics regarding • Support
6	Products / Standard software development
7	Solutions (customer projects)
8	Sales/Marketing

The exact responsibility is illustrated in the IS Board under Regulatory Areas.

3.1.4 Responsibility for QM

QM is mainly the responsibility of the employees as part of their roles. For each role, the responsibility for the quality of results is defined in accordance with the quality standards specified by the Executive Board.

Details can be found in the respective role descriptions and in the role concept of the AEB QM is performed by the respective roles according to the PDCA cycle:

- plan QM (do we even need a regulated process, rules and/or tools?)
- set up QM (is it a core process or accompanying process?)
- introduce QM (communicate, train, document, test)
- implement and embrace QM
- maintain and continuously improve QM (e.g. by regularly requesting internal audits and with the PDCA cycle).

QMS creates the necessary framework conditions for the QM core processes. Employees with the QMS Officer role manage it centrally and make it available to all employees. They accompany/coach and support employees who want to define measures, tools, trainings, etc. to assure quality as part of their role(s). By regularly exchanging information, they automatically create a transparent overview and a consistent documentation of the value-creating core processes. They provide trainings and communicate the “system”

both internally and externally (e.g. as part of tenders or external customer audits). They regularly check whether the system is adequate relative to the requested quality standard e.g. through internal audits or by deliberately pointing out existing contradictions. They support with their moderating influence, but do not take any decisions – but they request them continuously from the responsible parties.

Furthermore, the roles in charge of core processes and core topics practice quality management for their assigned core processes/topics. As part of this, they combine or synchronize and orchestrate the affected parties/roles to ensure that the quality standard necessary for our company success be achieved. Regarding QM, they consult directly with the QMS Officers.

3.2 Administration

For maintaining the management system and ensuring all related activities, tasks and resources (expenditures) are managed as projects in the ASSIST4CRM tool. These projects have the following characteristics:

- A runtime of one year.
- They specify roles; always at least a project manager and senior project manager
- Estimated expenditure

The required resources are determined and provided regularly. If required, corrections will be made. This guideline is published in the company's Confluence and communicated in a NEWS.

The guideline is regularly checked through:

- internal (regular) audits
- events, which change the application system or relevant boundary conditions

3.3 Competences and awareness

Responsibilities and competences are key elements in AEB's role descriptions. Assigning people to roles is a managed process. The roles descriptions are also subject to a managed process with role owners and verification by a second person for the release of roles.

All roles have the right to an adequate training and continuous training. The organization and its culture ensure that competence can be developed as employees gain experience in the network.

Important elements are knowledge of and familiarity with

- the objectives (i.e. in guidelines)
- the processes for achieving these objectives
- the provided tools, incl. documentation

Communication takes place in the form of discussions, meetings, training courses or within the framework of document control (e.g. via NEWS). The importance of observing or not observing the guidelines of the AEB is conveyed. It is emphasized that every contribution and the participation of each employee are important for shared success.

3.4 Communication

A lively management system requires communication. With a view to assuring quality, the following table provides orientation on how to inform actively:

When (cause)	What	Who	To whom	How
Change of specifications	Content of change, reasons	Person(s) responsible for specification (e.g. Board of Directors, QM)	QMS Responsible, affected employees	Email (and meeting); documentation in corrective and preventative measures
Change of organization	Content of change, reasons	Manager of the organization	QMS Responsible, affected employees	Email, intranet messages, follow-up training as needed
Change of guides	Content of change, reasons	Guide owner	Employees or concerned domain, relevant target group	Intranet news, follow-up training if required

Information is provided transparently in the company Intranet. Intranet news often refer to more detailed explanations in Confluence.

3.5 Documented information

3.5.1 General

To comply with general documentation requirements, the organization has created a documentation guideline.

See Document control (QMS).

Introducing and running a management system means the regular implementation of the PDCA cycle. This includes at least the following activities, which need to be documented:

- regular assessment and ongoing maintenance of the documentation required for the management system
- Seminars for training and continuous education are very important at AEB. All new employees have to attend mandatory trainings that are part of their onboarding process. For example, trainings that have a high significance for security are mandatory (workplace safety, data protection, data security, ISMS). More information can be found in Confluence in the Knowledge management section under: Security pyramid
- The audits – incl. internal audits – are logged.

3.5.2 Further regular activities

In the QMS

- Updating all rules and principles (1x/year)
- Updating the value-added chain and all underlying processes incl. roles (1x/year)
- Internal QMS audit after request by process owners

In the ISMS

- Repetition of risk assessment; at least 1x/year
- Maintenance of the risk treatment plan
- Maintenance of corrective and preventative measures
- Explanation of applicability (checking if everything is still up-to-date)
- Regular management evaluation
- Internal ISMS audit

In the DSMS

- Repetition of the data protection impact assessment; at least 1x/year
- Regular checks (e.g. on documents, procedure directory, conformity for data transfers to third countries with TIA (Transfer Impact Assessment) implementation)
- Release management coordinated with ISMS for the security concept; approx. 1x/year
- Regular reporting; at least 1x/year

4 PDCA in the IMS

4.1 Leadership

4.1.1 Leadership and commitment

From AEB's principles, from how we want to interact, and how we want to act in the market, our high quality, data protection, and security standards are derived. AEB's company management places a special emphasis on this and feels responsible for quality management, data protection, and security. Company management also wishes for all employees to be aware of this special responsibility and duty of care and for them to act accordingly.

Therefore, management systems for quality, data protection, and security have been set up, which fulfill the following criteria:

- compliant with the relevant ISO standards
- strategically integrated into the organization
- process-oriented alignment for continuous improvement to achieve the quality, data protection, and security objectives

The necessary efforts and additional resources will be provided for. Among other things, relevant roles have controlling responsibility. In addition to targeting objectives, an important aspect of the leadership task is encouraging all involved to contribute continuously to actual effectiveness and continuous improvement.

4.1.2 Guidelines on management systems

The associated guidelines are an integral part of the management systems. These guidelines fulfill the following criteria:

- compliant with the relevant ISO standards
- presentation of the objectives and their reasoning
- presentation of the application areas towards which the management systems are geared
- presentation of the organization which is dealing with the implementation of the objectives

These guidelines are subject to the processes for guideline documents. They are made in writing and their current version is made available to the employees for consideration.

4.1.3 Organizational tasks, responsibilities, and authorizations

An important part of the guidelines is the clarification of the organization with roles and their functions and authorizations. The objective of the organization is the continuous alignment with the objectives incorporated in the guideline, the development and adjustment to changing conditions. The management systems contain a check feature. As part of regular management evaluations, reports are made, decisions on upcoming correction and prevention measures are taken, and the measures are implemented.

4.2 Dealing with opportunities and risks

Whenever objectives are defined, you will also find conditions which might endanger or promote that the objectives are achieved. Looking at opportunities and risks is an important tool for increasing the reliability of the achievement of objectives. This consideration makes it possible to concentrate on the actual business objectives.

4.2.1 Considerations in the ISMS environment

Based on the guiding principles of the information security guideline, AEB operates an ISMS in which security risks are identified continuously according to a protection requirements analysis. Before a possible risk treatment is carried out, the adequate procedure is decided on in a regularly called management evaluation. Details, such as processes for risk assessment and risk treatment, are regulated in AEB's ISMS regulation document; see also ISMS Guide.

4.2.2 Considerations in the QMS environment

In the quality management environment, opportunity and risk are two sides of the same coin. A deep awareness of quality objectives sharpens the interest in achieving them. A deep awareness of possible risks, which might affect or prevent the achievement of quality objectives, helps making arrangements to increase the reliability with which objectives are reached. The same approach increases the opportunity of reaching

objectives. At the same time, managing risks in the QMS increases the chance of establishing trust in reliability and quality in the market.

4.2.3 Considerations in the DPMS environment

In the data protection environment, special consideration is required from the perspective of the data subjects. To this end, the mechanisms of the ISMS were largely adapted to the protection goal of the data subjects; both for the company's own employees as well as persons in the systems that are subject to commissioned processing under data protection law, among others. We regularly discuss the results of this in the data privacy impact assessment. A regulation for dealing with data mishaps has been established.

4.3 Planning for changes

In the course of regular internal audits we review once a year if QMS, DPMS, and ISMS are up to date, compliant and fit for purpose. For all information and definitions on how internal audits are carried out at AEB, refer here:

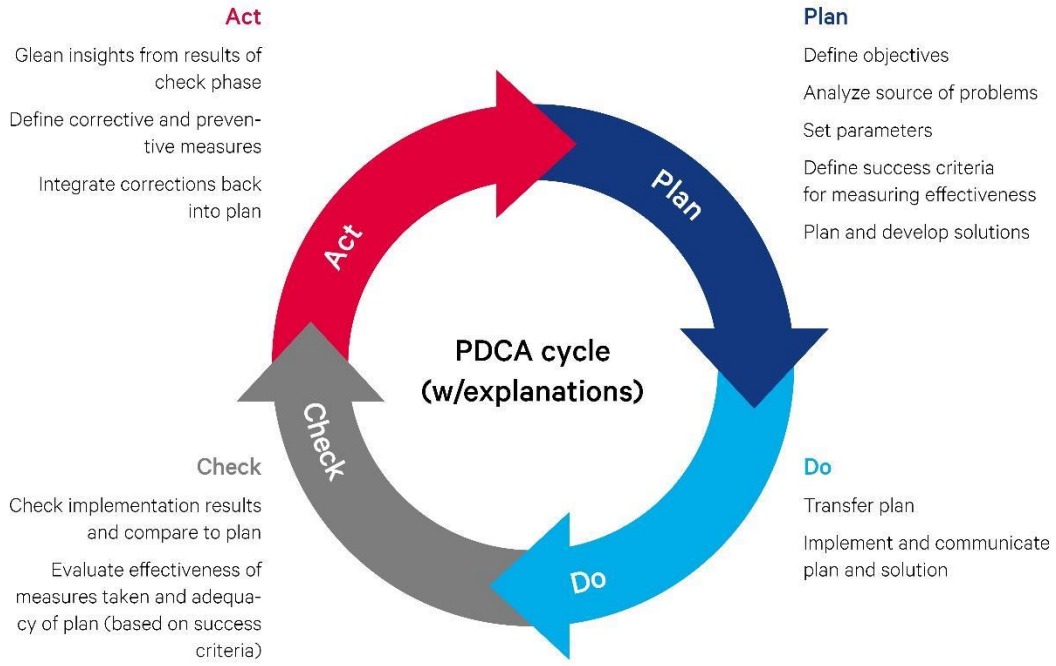
4.3.1 Certificates

The Certificates [EN] Confluence page lists all of AEB's certificates. In the Trust Center on the AEB website, all certificates as we provide them externally can be found.

4.3.2 Changes controlled by QM

The management systems are guided by the so-called Deming Circle, better known as PDCA cycle. This cycle describes an iterative, four-step problem-solving process as a classification for a continuous improvement. As described in theory, PDCA stands for Plan-Do-Check-Act and is based on the Gemba principle. The Gemba principle means “Go to the real place” where value-added processes in the company take place and where problems occur. Doing this puts the employees with their specific knowledge of the situation at the center of the planning. In sum, PDCA, the PDCA cycle, or PDCA management cycle:

- is a basic principle of a management system (for cross-divisional functions such as quality, data protection, or security)
- and stands for: "Plan, Do, Check, Act cycle". We therefore use this principle in
- our quality management (QMS) and
- our information security management system (ISMS).



This also includes:

- Changes in the IT landscape, in business processes, or threats and their evaluation must lead to a reconsideration of content correctness and meaningfulness.
- Changes of regulations and legal specifications
    - The Compliance Officer, Data Protection Officer, and Legal team have the particular obligation to inform.
    - Additionally, the following always applies: If legal requirements come to the knowledge of an employee by other means (e.g. announcements of the Chamber of Industry and Commerce or information research), they have to be passed on to the regular process via ticket to the Legal team or Security. If required, these cases are discussed further by the IS Board.
- Changes are introduced deliberately, with good reason, and in a comprehensible manner.

4.4 Meaning of the knowledge management for the IMS

Preserving and building up knowledge, distributing, and recovering it in a structured way is a constant challenge for companies with locations distributed across various countries. We meet this challenge with well-organized communication channels and filing systems, in addition to personal contact directly, by phone, or by e-mail.

Internally, a bilingual Intranet with Wiki system helps us spread news quickly and share knowledge with others. To the outside, we maintain various channels to the customer: Prospects and customers can get informed on our portfolio via our website www.aeb.com. Current topics are announced and put up for discussion via newsletter, in the Community and in the customer portal.

- More details on knowledge management can be found in the Knowledge Management section in Confluence.

4.5 Operations / use

The guideline's specifications have to be developed further and implemented. During this implementation, bear in mind the following requirements:

- Secondary documentation for implementation is also subject to the QM regulations
- This documentation has to be transparent and proves that the specifications are implemented (traceability, consistency)
- Control and documentation of changes

4.5.1 ISMS

- For implementing this guideline for information security, an ISMS Guide is available. It regulates, for example:
  - Risk assessment
  - Risk treatment

4.5.2 QMS

- The implementation of the QMS is described in detail under Quality management.
- For a short excerpt also on enforcement actions, see section Quality policy.

4.5.3 DPMS

- The implementation of the DPMS and its maintenance is explained in detail on AEB's internal Data Protection Management System page.
- The Data Protection Guideline is available in the AEB Trust Center (access point "Data Protection").

4.6 Ensuring control and effectiveness

Question/objective: How can we ensure that we keep an eye on requirements, which are put on the respective management system?

The management system guideline presents the organization and roles, which have the relevant powers and controlling responsibility in the management system. Ensuring effectiveness builds the bridge between theoretical planning and implementation to promote that objectives are achieved. Building this bridge is part of the management's self-commitment.

Additionally, the processes and tools include checks, which ensure that objectives are achieved while taking target criteria into account. Example: Employees with a dedicated partner manager role are taking care of partnerships (service providers, suppliers, development partners, sales partners) throughout the entire lifecycle.

Furthermore, the following tools serve to ensure the effectiveness of the quality measures:

Tool	Relevant roles	Indicators and scale in effectiveness test
Executing all tasks, including the "quality" and "security" long-term tasks, as projects with sets of measures, assignment of responsibility,...	Senior project manager, project manager, project member	RFD (looking at resources, function, date); regular appointments with the senior project manager, holding a PEM if necessary
For more complex or challenging projects holding project meetings at the beginning and end; influencing project characteristics; working with milestones	Project team, company management	RFD; looking at opportunities and risks
Working with appointment series with an agenda on task grids	Organizer of the appointment, participants	Feedback culture (participation, number, and content of feedback)
Evaluation meetings on KPIs; also for presentation and discussion in the management evaluation; clear structure of management evaluations, which is also regularly checked for appropriateness.	Management "management system", top management	List of relevant KPIs; queries; statistical evaluation of trends
Feedbacks integrated in training programs	Continuous training, trainer	Open, anonymous, unorganized feedback (usually provides statements on satisfaction, comprehension, awareness of transported content)
Internal and external audits	Auditors, process participants	specification of guideline documents on management system; feedback rounds; quality of the internal audit, guide which also provides for getting feedback.
Controlled communication	Authors	Specifications, e.g. guideline documents, instructions for use
Integrated risk management	Project Manager, Senior Project Manager, ISMS Manager, Data Protection Officer	Checklists to encourage to think about risks, which could endanger the objectives.
Risk treatment	Domain Safety Officer, risk owner	Integrate section in risk treatment Define risk indicator(s), which express the occurrence of the risk. Example: Number of tickets with defined symptom.
Customer surveys, getting feedback	Marketing, service organization	Action-driven questionnaires; evaluation

4.7 Improvement

The last phase "act" or improvement closes the cycle for the regulated iterative process by implementing insights from operating the management system and correcting the specifications accordingly.

Therefore, the respective insights have to be

- documented and analyzed,
- examined for causes of errors, for example, and
- developed to become ideas for corrective and preventive measures.

The corrective and preventive measures have to be

- documented,
- transferred into adjustments of the specifications, and
- forwarded to the employees concerned.

4.7.1 Further important documents

- Security Guide
- ISMS Guide
- QM Guideline
- Data Protection Guideline