Manual

Guideline Integrated Management System (IMS)

13.12.2018

Content

Note: In this documentation there are some Links, which enable AEB employees to open up further informations in AEB Intranet. This illustrates the high level of integration in AEB's knowledge management.

1 Guideline and rules on policy of quality and information security

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 revised ISO 9001 and ISO 27001 standards since 2014.

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 • Competences • 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 quality and security
- 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 and security here. For specific statements on quality 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 and information security (framework for defining objectives, principles of action, etc.) For orientation, we rely heavily on **ISO 9001** and **ISO 27001**, for which we have been certified since February 2010.

- Rules keep changing; we live in a dynamic world.
- First and foremost, quality and security mean awareness.
- Quality and security are a claim whose realization has to be trained.

  Therefore, we see quality management as a commitment, a general attitude, and a process of continuous improvement. We are oriented towards long-term relationships. We perceive security to be a part of or perspective on quality.

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; e.g. legal compliance	Contractual commitment (license, support, SLA, NDA); statements in system descriptions	Product management, legal, service organization (e.g. SLA management)
Legislature	Compliance	Transfer through training, for example	Legal team; 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

Further explanations:

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 hosting solutions also require us to fulfill security and quality demands resulting from legal requirements for our customers and their processes. AEB ensures a high degree of compliance of security standards due to its role and activities as service provider in the context of its industry environment. The growing challenges in the face of internationalization necessitates the orientation on internationally recognized standards. The quality standard is immediately derived from the conditions and requirements for using the products. AEB deems the security perspective an increasingly critical decision criterion in the market. Security in this sense means more than just mastering the technical facets. It includes 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.

Legal requirements

With short description in key words:

- KonTraG (requirement to implement a monitoring system; early detection; statements on risk structure; proof of traceability on functioning of a control system)
- GDPdU, 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)
- BDSG (provision of a security concept as outlined in section 9 – technical and organizational measures; due care concerning personal rights of persons concerned, data minimization, confidentiality)
- Basel II (indirectly via requirements to banks as lendors)

- **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.

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 Federal Data Protection Act (BDSG) specifies requirements on special duty of care when dealing with customers, partners, and subcontractors (see data processing as defined by section 11 BDSG). A data protection officer has been appointed.
- Conclusion of nondisclosure agreements (NDA) with business partners (customers, partners, subcontractors); internally, employees are bound to section 5 BGSG (data secrecy), and are made aware and trained in the confidential handling of information.
- With subcontractors, NDAs are concluded; 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.

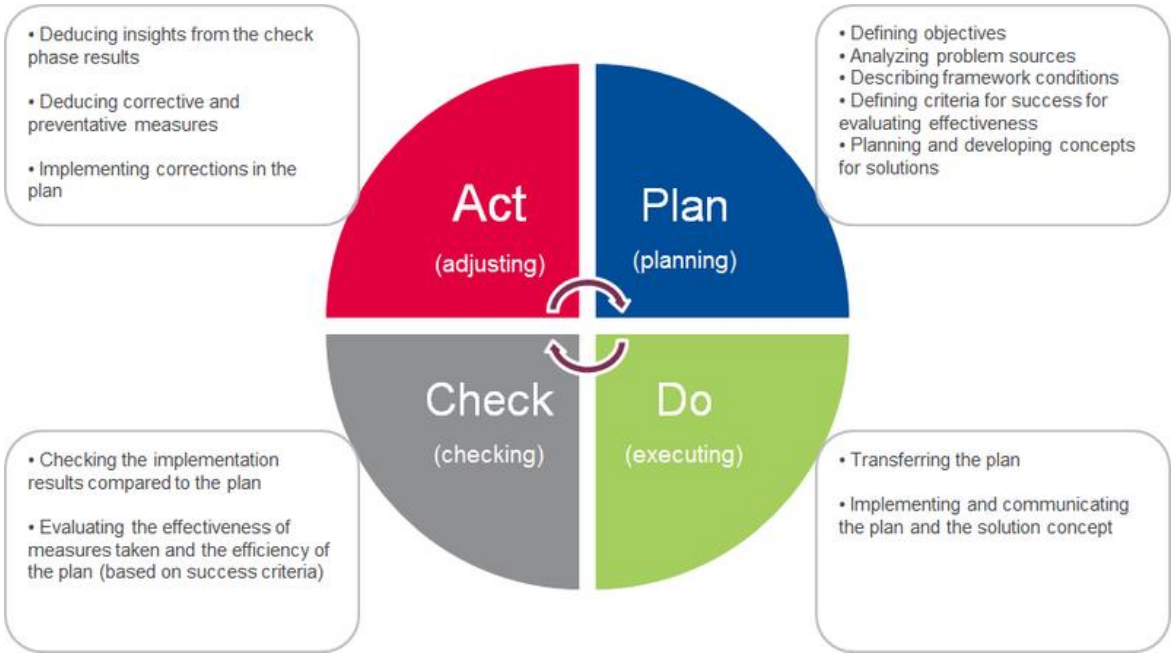
Other regulatory requirements

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 modules,
- are monitored continuously in meetings of the IT Security Board or the QM Steering Committee, and
- are checked regularly during internal audits.

To ensure sustainability (effectiveness of ISMS and QMS)

- a PDCA cycle has been defined which also include responsibilities and rules



- all employees are asked to turn to the IT Security Board if changes occur in the environment, which will affect security-related aspects
- the specifications of the ISO 9001 and ISO 27001 standards and our rules for the corresponding management system provide orientation

1.3 Application areas

On ISO 9001 – procedures and processes

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

- all locations
- all products

Reason for the selection

With the increasing importance of software and services for the value-added processes of companies (AEB customers), their demand for the quality of AEB's software products also rises. For AEB, it is important to convince customers with solutions and services which will satisfy their expectations in the long-term and meet the highest quality standards.

On ISO 27001 – procedures and processes

The application area is the AEB customer data center in Colocation / Stuttgart.

- Location: Stuttgart-Vaihingen, Breitwiesenstrasse
- System: Hosted systems (operation and services) for our customer, available for all our applications of the ASSIST4, ||XPRESS, Engines, ATC product series.
- Interfaces: These are access systems for remote access (CITRIX server, WebServer for Internet connections,...), connections with customs, for example. Adjacent system are the following:
  - Service/support: Change management process
  - Products/customer projects: Release management process

- Facility management customer data center
- Additional services by partners: Partner management process, for access with partner contracts for system access

Reason for the selection

- Start of the certification efforts concentrating on a core (allowed by ISO, enables modular approach)
- High protection need for operating the data center
- The customer data center is a significant part of our business
- We have therefore deliberately selected a large and signification application area as "pilot"
- We are aware that this concentration can only be the beginning

A more detailed list of the assets (in the course of inventory) and risks will be made in a separate, specifically provided tool (RiscTool) on risk management.

2 The QMS and ISMS management systems in the IMS

Process-oriented management systems ensure operation and continuous improvement.

This includes the following, for example:

- 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 AEB quality standard

AEB's quality standard is based on the AEB Magna Carta and was worked out by the Quality Management Team in cooperation with the Executive Board. Defined quality criteria make the standard comprehensible. They describe transparently AEB's expectations towards solutions, services, company-wide cooperation, and finally every employee.

Quality standard

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

AEB's quality standard aims at...

- Introduction of solutions that satisfy our customers' requirements and delight them.
- Development of integrated software products with a high usability which fulfill the needs of the market at reasonable prices, are easy to install, roll out, and operate.
- 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). We handle customer data and wishes securely and confidentially.

- Successful and satisfactory projects (customer projects and internal projects) are completed 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 to allow both sides to engage in a sincere and professional cooperation.
- Successful, sustainable marketing of our products and the company.
  A This also involves a respectable, competent, and transparent communication with the market and our discussion partners. Reliability and requirements traceability from proposal to order
- Efficient & transparent administration
  An efficient and transparent administration which ensures compliance with official regulations and agreements. Streamlined processes in commercial transactions closely interconnected with other areas.
- Transparent and reliable Employee Services which promote every individual's wellbeing and work in joint efforts with the team leaders at the company.
- Ensuring high quality levels of training and continuing education to keep internal knowledge and competences at a high level.

Objectives are therefore...

- Successful and sustainable marketing of the products and the company

  This is made transparent by:
  - Reliable, competent, transparent communication with the market and our partners
  - Reliability and requirements traceability from proposal to order
  - Distribution processes guided by high service quality
  - Secure and confidential handling of customer data
- Development of integrated software products with a high usability which fulfill the needs of the market at reasonable prices, are easy to install, roll out, and operate.

  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 software (friendly, ergonomic, intuitive, tangible, and easy to use)
  - Striving for accuracy (every line of code is approved and tested)
  - Securing compatibility in the system landscape
  - Ensuring an easy installation
  - 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

- Integrated, comprehensive services (service products) and 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
- 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 interconnected with the other departments
  - 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

Quality policy

AEB's quality policy is based on the company manual.
In essence, the QM assumes responsibility for the following topics and pursues the following objectives: It is always our goal to ensure our value-adding business operations or process. Our value creation from service and software products 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 are based on an integrated role concept that strengthens and supports the personal responsibility of each employee in the company's value chain.
QM is practiced as part of each employee's role(s) – within the framework provided by the QMS.

AEB's underlying principles are the following:

- Professional 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

Our most important security criteria 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 made in the form of default contracts or separately in SLAs. 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/IKS) was 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)

Generally, we are aiming at pursuing the **principle of the outer perimeter defense** as a security strategy. The boundary to be defended is oriented towards the selected application area. We look at this security strategy in the risk assessment phase. 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 is to help improve handling confidence and make the risk handling process more efficient (in-depth research or acceptance of risk). The ISMS should be suitable to achieve the security goals 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. We believe that operating the ISMS will increase the motivation of our employees since they will recognize the importance of information worth protecting (assets) for our organization, for internal and comprehensive processes. As from a quality perspective, employees are made more aware of security issues through trainings, for example, and become more involved by assuming responsibility.

An important aspect are intensive efforts to prevent problems, for example:

- Various regular checks, and internal and external audits. To test our security, we simulate internal and external attacks regularly. We have assigned an external service provider to carry out these penetration tests.
- Early detection principle (monitoring and alerting of the systems)
- Thorough follow-ups, analysis of causes when emergencies have occurred
- Operation of an emergency concept and an emergency organization
- Performance of emergency drills (based on simulated scenarios)
- Keeping security awareness alive actively (Intranet, trainings, etc.)

Security – the most important rules

The Security Guide in English 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

- Observing data protection (internally and externally)
- Regular participation in trainings (on security awareness)
- Dealing with personnel
- Ensuring that nondisclosure agreements are concluded with business partners if necessary

3 IMS organizational structures

3.1 Roles, responsibilities, and resources

Introduction

AEB uses a distinctive roles concept. 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.

Relevance in management systems

Our roles are the following – in order of management system relevance:

Role	Capacity, responsibility	Member in	Comment
Managing 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		Highest responsible body
QM Steering Committee	Exchange; clarifying comprehensive matters / see also *QM organization*		regular meetings in appointment series
Quality manager	QM responsibility per domain	QM Steering Committee	one quality manager per domain
Manager IS Board (security management)	• Managing the Board • Controlling the ISMS according to our specifications, particularly if regular activities are observed	IS Board	Operating the PDCA cycle on ISMS operation; also participant in

	• Initiating internal audits • Monitoring work on the risk treatment plan • Evaluating the effectiveness of measures • Creating an explanation of the applicability • Documenting management changes • Ensuring document guidance • Reporting on security incidents • Offering modules on security training and ISMS awareness • Initiating and monitoring security checks		the Security Working Group
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	preferably, this role is assumed by quality managers
Management "System Management"	• IT infrastructure	Security Working Group	only partially included
IT Operations	• Operating the data center • Co-responsible for Business Continuity Management (BCM)	Security Working Group	details defined in Service Guide
Every member of the IS Board or QM Steering Committee	• Preserving contacts with authorities and security-relevant interest groups	IS Board; QM Steering Committee	
Product manager Services	• Co-determining tolerable risks for customer installations	Security Working Group	only called in on an case-by-case basis

	• Knowing about existing SLAs and the agreed customer demands		
Data Protection Officer	• Working towards compliance with the Federal Data Protection Act (BDSG)	Security Working Group	only called in on an case-by-case basis

Notes on the ISMS

The approval of the management on the ISMS guideline also signifies their general approval of the identified risks that will be accepted. Various roles in the IS Board assume responsibility for information security at AEB. As a rule, we want to work with roles. The current entities can be found in the organizational structure according to the valid documentation. There is a designated person responsible for IT security, appointed by the management (IT Security Manager). In close cooperation, a ISMS Manager is responsible for operating the ISMS.

Domain Security Officers, owners, and responsibility

Organizationally, we want to keep the operation of the ISMS as lean as possible. The role of Quality Manager (QM) is therefore co-responsible for information security. 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.

The ISMS document 'Explanations on applicability' regulates the details and the detailed assignments. Every line (regulatory area – security category – measure objective) is assigned to a responsible person. The Domain Security Officers regularly check the documentation relevant for their field of action for their responsibility and the realization of the measure objective.

Nr.	Domäne
1	**Administration** with topics on • Law, compliance, data protection • Commercial processing, controlling
2	**HR department** (Personnel)
3	**Infrastructure** with topics on • System management; • Building services
4	**Services** with topics on • IT Operations (operation, communication); • Support
6	**Products** / Technology for use

7	**Solutions** (formerly: customer projects)
8	**Sales/Marketing**

The exact responsibility is illustrated in *IS-Board*.

Responsibility for QM

As specified in the definition, QM is mainly the responsibility of the employees as part of their role(s). For each role, the responsibility for the quality of results is defined in accordance with the quality standards specified by the Executive Board. For details, refer to the corresponding role descriptions and the AEB role concept. In accordance with the PDCA cycle, the corresponding roles:

- 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).

As specified in the definition, QMS creates the necessary framework conditions for the QM core processes. Employees with the Role: 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 with each other, 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, 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 WIKI 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 in the form of conversations, meetings, trainings, or document guidance (per NEWS, for example) must deepen the significance of complying with or not complying with the AEB guidelines. 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	Whom	How
Change of specifications	Content of change, reasons	Person(s) monitoring specification (e.g. Executive Board, QM	QMS Officers, affected employees	E-mail (and meeting); documentation in corrective and preventative measures
Change of organization	Content of the change, reasons	Manager of the organization	QMS Officers, affected employees	E-mail, NEWS, if required follow-up training
Change of guides	Content of change, reasons	Guide owner	Employees or concerned domain,	NEWS, if required follow-up training

			relevant target group	

Information is provided transparently in the company Intranet (WIKI). NEWS often refer to more detailed explanations in WIKI.

3.5 Documented information

General

To comply with general documentation requirements, the organization has created a documentation guideline. For details, see *QM:Rules for QM documentation*. 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 called "modules" at AEB. All new employees have to attend mandatory modules that are part of basic training. For example, modules that have a high significance for security are mandatory (workplace safety, data protection, data security, ISMS). Find further information on the wiki in the continuous education category (in German).
- The audits – incl. internal audits – are logged.

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

4 PDCA in the IMS

4.1 Leadership

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 and security standards are derived. Company management places a special emphasis on this and feels responsible for quality management and security. Company management 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 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 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.

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.

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 explicitly 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.

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 *QM:ISMS* Guide.

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.

4.3 Planning for changes

In the course of regular internal audits we once a year if QMS 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: https://service.aeb.de/en/open/guidelines-and-certificates/

Certificates

The Certificates wiki page lists all of AEB's certificates. On the AEB website, all certificates as we provide them externally can be found at

Changes controlled by QM

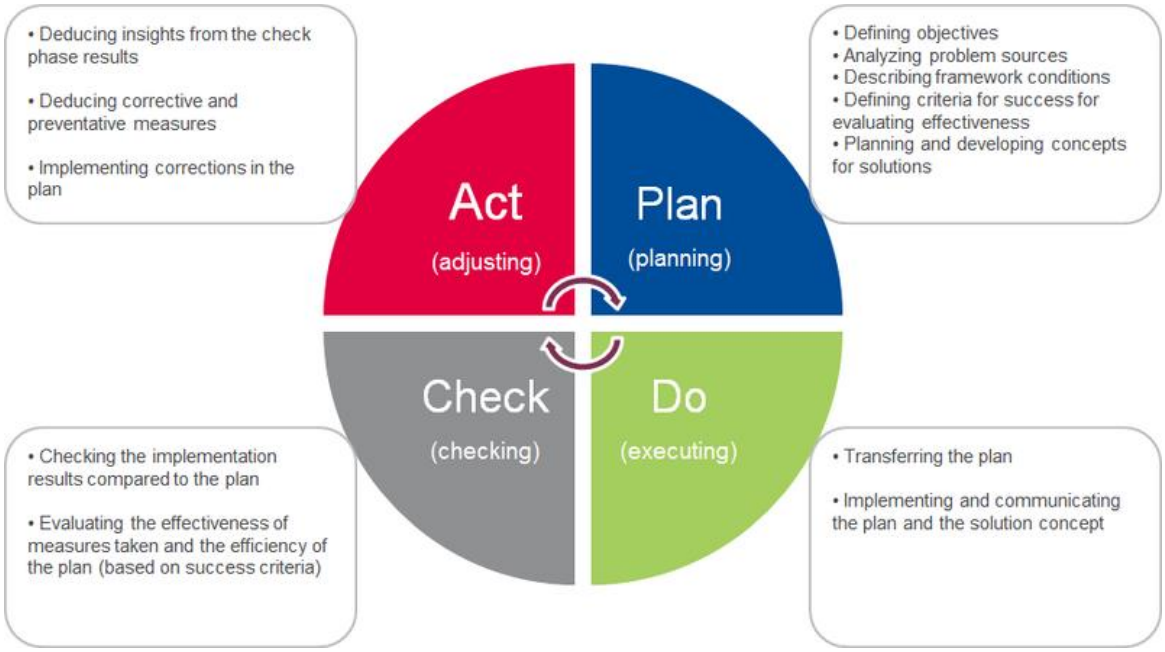
Within the scope of its work, Quality Management is guided by the so-called Deming Circle, better known as PDCA cycle. This cycle describes an iterative, four-step problem-solving process as a classification for a continuous improvement. As described in theory, PDCA stands for Plan-Do-Check-Act and is 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 or security)
- and stands for "Plan-Do-Check-Act cycle"

We therefore use this principle in the following areas:

- our quality management (*QM: Quality management*)
- our information security management system (ISMS)



See also *QM Methods & Standards.*

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 support case to the Legal team or the Security Working Group. 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 and in the customer portal.

For more details on knowledge management: *QM:Knowledge management*.

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

ISMS

For implementing this guideline for information security, a *QM:ISMS Guide* is available. It regulates, for example:

- Risk assessment
- Risk treatment

QMS

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

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 *Role: Partnermanager* 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, Executive Board	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 (Company Management)	list of relevant KPIs; queries; statistical evaluation of trends
QA checks according to corresponding check lists	Person responsible of the process (e.g. partner management)	check lists indicate targets or consequences
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, domain quality managers	specification of guideline documents on management system; feedback rounds; quality of the internal audit, guide which also provides for getting feedback.
Controlled communication	authors such as domain quality managers	specifications, e.g. guideline documents, instructions for use
Integrated risk management	Senior project manager, project manager, domain quality manager	Check lists to encourage to think about risks, which could endanger the objectives

Risk treatment	Domain Security Officer, risk owner	Integrate section in risk treatment Define riks indicator(s), which express the occurrence of the risk. Example: Number of support cases with defined symptom.

The QMS and ISMS management systems

Process-oriented management systems ensure operation and continuous improvement. This includes the following, for example:

- the guideline for clarifying objectives and organization
- tools for monitoring of effectiveness
- administrative tools and process-oriented working for operation, monitoring, and improvement
- risk management
- be aware of customer requirements, customer satisfaction…

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.

Further important documents

- *QM: Security Guide*
- *QM: ISMS Guide*
- *QM: Quality management*