

BVMed Compliance Standard



Legal Notice

© Copyright by
BVMed - Bundesverband Medizintechnologie e.V.
Reinhardtstr. 29 b, 10117 Berlin
Tel.: +49 (0)30 246 255-0
Email: info@bvmed.de

[September 2021]

Reproductions, including excerpts, are only permitted with the express permission of BVMed.

The development of the BVMed Compliance Standard and the samples was supported by Dr Peter Dieners and Ulrich Lembeck (both from Clifford Chance Partnerschaft mit beschränkter Berufshaftung).

Reliable points of reference

Foreword

BVMed Compliance Standard

Standard for the compliance organisation of medical device companies, medical aid providers and homecare providers and their self-review through an internal compliance system audit.

This BVMed Compliance Standard offers reliable points of reference for governance-related compliance questions as well as practicable suggestions and tips for setting up a suitable compliance organisation.

The Bundesverband Medizintechnologie e.V. (BVMed) published the Medical Devices Code at the end of the nineties and has continued to develop it ever since. The aim of this code is to explain the legal framework of cooperation between medical institutions, physicians and manufacturers of medical devices. The Medical Devices Code summarises the existing legal provisions and contains rules of conduct that should be observed in cooperation. Since its publication, it has been widely acknowledged among all relevant stakeholders as a reliable point of reference with regard to behaviour-related compliance issues in the medical device industry. The member companies of BVMed promote consistent adherence to the compliance requirements by creating organisational framework conditions in the companies. The importance of the organisational framework conditions can also be seen from the large number of domestic and foreign regulations that require companies to take appropriate organisational measures to prevent compliance violations. It is true that in Germany there is no explicit legal obligation to appoint compliance officers or to set up a compliance management system for the medical device industry (in contrast to certain other industries such as the finance or insurance sectors). However, according to the case law on Section 43 GmbHG, Section 93 AktG as well as Section 130 OWiG, it is part of the duty of care of the company management to take appropriate measures to control compliance risks. As a general rule, this also includes the appointment of compliance functions if the company management does not perform these itself, as this may well be permissible and practical in the case of very small companies. The lack of any measures in the event of compliance violations can have an aggravating effect on government sanctions against the companies themselves and their employees or management levels.



Dr Marc-Pierre Möll
Managing Director of BVMed

BVMed Compliance Standard

Compliance organisation of medical device companies and their self-review

Contents

Foreword	3
A. BVMed Compliance Standard	5
1. Compliance understanding and value basis	6
2. Establishment of compliance positions	8
3. Compliance risk analysis	10
4. Whistleblowing system and assistance in compliance matters	12
5. Rules and processes	14
6. Training courses	16
7. Compliance audits and self-reviews	18
8. Corrective measures and continuous improvement	20
9. Internal investigations and sanctions	21
10. Documentation of the compliance organisation and its modules	23
B. Self-audit of the compliance organisation	25
1. Subject of the self-review	26
2. Procedure of the System Audit	26
3. Benchmarks for the System Audit	27
4. Audit report	28

Benchmarks and industry best practice

Against this background, there is an increased need on the part of companies to obtain reliable points of reference for organisation-related compliance topics as well as practicable suggestions and tips for setting up a suitable compliance organisation. This applies in particular to small and medium-sized companies in the sector which also want to meet the growing requirements without being overwhelmed by complex organisational structures. The BVMed Compliance Standard is therefore primarily aimed at small and medium-sized companies.

Clarity on the essential elements of a compliance organisation

The BVMed Compliance Standard

- > is based on the relevant legal requirements in Germany regarding the duty of care of company management, in particular in connection with Section 43 GmbHG, Section 93 AktG and Section 130 OWiG and their interpretation by case law and the existing national and international standards;
- > describes the essential elements of a suitable compliance organisation and is intended to enable companies in the medical device industry, providers of medical aids and homecare providers to take organisational precautions that are in line with today's common and generally accepted benchmarks and industry common practice;
- > contains benchmarks and criteria for how companies can ascertain by means of a self-review through an internal compliance system audit that the measures they have taken are in line with these requirements.

A. BVMed Compliance Standard

The essential elements of a suitable compliance organisation are illustrated in the following modules:

1. Compliance understanding and value basis
2. Setting up compliance positions
3. Compliance risk analysis
4. Whistleblowing system and assistance in compliance matters
5. Rules and processes
6. Training courses
7. Compliance audits and self-reviews
8. Corrective actions and continuous improvement
9. Internal investigations and sanctions
10. Documentation of the compliance organisation and its modules

1. Compliance understanding and value based

A. WHAT DOES COMPLIANCE MEAN AND HOW FAR DOES IT GO?

Compliance does not only mean the observance of all laws by a company, its employees and commissioned third parties (e.g. service providers, consultants or agencies), because conduct in conformity with the law is a matter of course. Rather, compliance also includes acting in accordance with voluntary commitments, internal company policies, guidelines and requirements. Voluntary commitments routinely include a commitment to adhere to certain values.

“Correct” behaviour requires clear values. Therefore, a company should clearly express its ideas of what it means to act in ethical manner and to have integrity and which values it wants to pursue (compliance understanding).

B. HOW AND WHERE IS THIS IMPLEMENTED?

Value concepts are laid down in policy documents of the company, for which different terms are often used in practice. Terms such as “Code of Conduct”, “Our Values”, “Compliance Guideline” or “Purpose Statement” etc. are frequently used. In order to convey the company’s own understanding of compliance, guidelines and instructions that are important for compliance routinely refer to such policy documents.

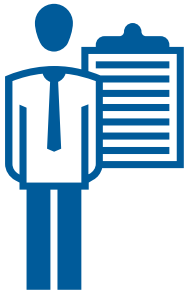
An example of a code of conduct with topics and headings typical in the medical device industry can be found in the [Code of Conduct Annex](#). This also contains a sample wording for the reference to the values pursued by the company in a compliance organisational guideline (reference/link to module 10 point c.).

C. EXAMPLE SETTING AND TONE FROM THE TOP

The conviction that all levels of management are serious about compliant behaviour and business integrity is a key factor in encouraging employees to do the right thing. To achieve this, the importance of the compliance culture and compliance awareness must be continuously maintained and renewed (also called “tone from the top”). This can be done in company, departmental or committee meetings, compliance messages/communications or in other communications expressed by the management levels on compliance cases and aspects. It must be clear from these that compliance is taken seriously by them personally and by the company in every respect.

*Seriousness is
also expressed
in resources*

Seriousness is also expressed in the resources made available for compliance. It is also reflected in the consideration of compliance aspects when granting incentives and incentive-based remuneration to employees, e.g. when the achievement of certain sales targets is not the only factor influencing an annual bonus. For example, special compliance efforts can increase an annual bonus or lack of participation in compliance training can reduce it.



D. REQUIREMENTS SPECIFICATION: WHAT WILL AN AUDITOR ESSENTIALLY WANT TO KNOW?

- i. Has the company clearly defined and published its compliance understanding and values?
- ii. Does the company make it clear through its representatives that it is serious about its commitment to compliance and business integrity?
- iii. Does the company take appropriate measures to continuously deepen the understanding of its employees and commissioned third parties for value-based actions and the importance of compliance?

2. Setting up compliance positions

A. WHAT IS THE IMPORTANCE OF COMPLIANCE OFFICERS?

The responsibility for compliance itself, i.e. the adherence to all relevant legal and internal requirements, is an essential responsibility of every employee. However, the management has the task of establishing and maintaining a functioning and sustainable compliance management system that supports the employees in doing so. This task is routinely assigned to one or more compliance officers, who are responsible for the compliance organisation in the entire company or group of companies after the duties have been assigned accordingly. In smaller companies, the task is often also assigned to a single member of the management.

B. COMPLIANCE OFFICERS

Typical persons responsible for compliance are compliance officers and a compliance committee. Depending on the size, structure and risk exposure of a company, additional compliance officers may be required, e.g. regional or local compliance officers, centralised compliance focal points or offices, etc. In the medical device industry, taking into account its specific risks, additional special compliance functions may be considered, for example to ensure sufficient separation of medical research/development and marketing/sales (separation principle).

C. DELEGATION OF COMPLIANCE RESPONSIBILITIES/DUTIES, AUTHORITY AND REPORTING LINES

In order to protect the company, its employees and management levels as much as possible, it is important that the duties of the compliance officers be defined in detail and that they be legally binding. Examples of a delegation letter and the essential duties of a compliance officer can be found in the **Delegation Letter Annex**. In order for compliance officers to be able to perform their duties efficiently, they need sufficient independence and authority, for example to be able to investigate compliance cases without being influenced. Their reporting channels, the degree to which they are dependent on instructions and the conditions under which they can be called up or dismissed must be defined in detail. The top compliance officers must have direct access to the management and, in the event of discrepancies with the management, to any existing supervisory bodies for reporting purposes. Independence granted in accordance with this requirement and an appropriate budget allow for a sustainable and serious promotion of the idea of compliance.

Protecting the company, its employees and management levels

D. CONNECTION AND INDEPENDENCE

In larger companies, compliance responsibilities are routinely part of an independent department. However, this is not necessarily mandatory. In smaller companies, a connection to the legal department, the internal audit department or the like can be considered. In any case, a clear demarcation from other functions must be formulated. The Annex contains an example of the demarcation of compliance responsibilities from the legal department.

E. REQUIREMENTS SPECIFICATION: WHAT WILL AN AUDITOR ESSENTIALLY WANT TO KNOW?

- i. Has the company established compliance responsibilities that, by their nature, number, equipment and suitability, are capable of establishing and maintaining a functioning and sustainable compliance management system appropriate to the size and risk exposure of the company?
- ii. Are the duties of the compliance officers defined in detail and legally binding on them?
- iii. Do the compliance officers have sufficient independence and authority? Are their reporting lines and the degree of their dependence on instructions defined in detail? Do the top compliance functions have direct reporting access to the management?

*Central
element of
every
compliance
programme*

3. Compliance risk analysis

A. WHAT DOES IT MEAN ?

Conducting a compliance risk analysis (also called compliance risk assessment) is the central element of any compliance programme. This is because it is necessary to determine all risks that are particularly serious from a compliance point of view, i.e. the compliance-relevant risks, and to assess them with regard to their damage potential and their probability of occurrence. Only on this basis can the appropriate measures be taken to deal with them or to mitigate them.

B. METHODOLOGY

In principle, there are no guidelines for medical device companies as to what the methodology is for a compliance risk analysis. The decisive factor is that the method chosen by the company is suitable for identifying as many existing and emerging compliance-relevant risks as possible. The **Risk Matrix Annex** contains an example of a simple list (risk matrix) of possible compliance-relevant risks. The example can be a starting point for a compliance risk analysis, whereby the list is refined, completed and further developed with the involvement of other bodies in the company. In addition to the complete recording of compliance-relevant risks, the compliance risk analysis also includes the quantification of the risks, essentially depending on the possible extent of damage, their probability of occurrence and the frequency of their occurrence. Finally, the measures taken to mitigate with the risks must be assigned to the risks. If it becomes apparent that the measures taken (guidelines, instructions, processes, etc.) are either not suitable, not effectively implemented or not complete, action must be taken to remedy this.

C. HOW OFTEN AND BY WHOM?

The risk analysis must be repeated regularly, unless there is an acute need to update it, e.g. due to a change in corruption laws or the like. In principle, it is sufficient to update the risk matrix on an annual basis once it has been drawn up. With the broadest possible participation of relevant employees who are responsible for the respective matter ("risk owners"), a "risk map" is created. This gives the company a clear orientation at all times. It can also contribute to a successful defence in possible investigation proceedings. The responsibility for managing and supervising the risk analysis routinely lies with the compliance officers. The company must determine which other departments in the company are involved in its implementation (e.g. internal audit, risk management, management levels of the business).

D. PERSONAL BEHAVIOUR AND ORGANISATIONAL RISK AREAS

The risk matrix included in the [Risk Matrix Annex](#) as an example shows, among other things, the risk areas that typically arise in the medical device industry when companies work together with healthcare professionals. In addition to the risks that may arise, for example, from the behaviour of sales representatives or members of medical departments, the risk analysis must also take into account those risk areas that may result from an inadequate or faulty organisation of the company. This may include an inadequate design of the compliance organisation as well as risks in connection with complex group or matrix structures. These can arise in particular from faulty delegation, unclear competences and unregulated responsibilities.

E. REQUIREMENTS SPECIFICATION: WHAT WILL AN AUDITOR ESSENTIALLY WANT TO KNOW?



- i. Has the company defined the criteria it uses to classify risks as compliance-relevant?
- ii. What methodology does the company use to identify all existing and emerging compliance-relevant risks?
- iii. According to which standards does the company evaluate or quantify identified risks?
- iv. Where are the measures and controls taken (guidelines, instructions, processes, etc.) to mitigate identified compliance-relevant risks described and presented?
- v. By whom, at what intervals and on what occasions is a risk analysis performed?

4. Whistleblowing system and assistance in compliance matters

A. WHY ARE THE WHISTLEBLOWING SYSTEM AND ASSISTANCE IMPORTANT?

A central element of an efficient compliance organisation is a whistleblower system. This is because compliance violations can only be remedied by a company if the competent bodies become aware of them. It is equally important that employees can also receive clear guidance on all compliance related questions through trustworthy advice.

B. AUTHORITY

In addition to the employees' superiors, the compliance officers of a company are generally the right contact persons to advise employees on all compliance issues. They also routinely have the authority to take or initiate the necessary measures to clarify suspected compliance cases that have come to light and to remedy violations. It is essential for the efficiency of an internal whistleblowing system that the employees be informed about this in an appropriate manner. In addition, it should be credibly communicated to them and the practice should be embodied in the company that reporting compliance violations or suspicious cases will not lead to negative consequences under labour law or career losses.

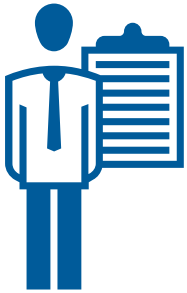
C. BASIS OF TRUST AND RULES

Confidence in an internal whistleblowing system and the absence of adverse consequences in the event of questions or reports of any kind can only be achieved through a clear commitment on the part of company management. Accompanying organisational measures are also necessary. These include the establishment and publication of information and rules on

- > which issues will be dealt with by the whistleblowing unit and when it can be contacted;
- > how whistleblowing is handled (software tools);
- > what level of confidentiality is guaranteed and how to communicate with the whistleblower (language, channels);
- > which measures are taken to check the plausibility and clarify tips;
- > the extent to which information and findings are documented and which departments in the company are allowed access to them.

The establishment of comparable rules is also recommended for advice and assistance in compliance matters.

Dealing with reports in an open and trustworthy manner



D. ANONYMOUS REPORTS

The efficiency of a whistleblowing system depends to a large extent on a corporate culture that promotes an open and trustworthy approach to whistleblowing. Above all, it is therefore advisable to further develop the corporate culture in this respect and to strengthen trust in open reporting possibilities. If a company considers the opening of anonymous reporting possibilities to be sensible or unavoidable, it is free to either set up an internal whistleblowing unit with anonymous reporting possibilities or to commission an external contact point (ombudsman, lawyer of confidence, whistleblower hotline or the like). An internal solution requires special rules to guarantee the anonymity and independence of the internal whistleblowing unit.

E. REQUIREMENTS SPECIFICATION: WHAT WILL AN AUDITOR ESSENTIALLY WANT TO KNOW?

- i. Has the company established clear rules for a whistleblowing unit and compliance advice and communicated them in such a way that all addressees have easy access?
- ii. Through what means of communication and complementary organisational measures does the company and its management credibly convey that reporting compliance violations or suspicions will not lead to adverse labour law consequences or career losses?
- iii. What rules apply to the handling and clarification of tips as well as the implementation of consultations?

5. Rules and processes

A. IMPORTANCE OF RULES AND PROCEDURES

Legal regulations alone do not routinely provide clear guidance as to which behaviour in the specific situation of an individual case is to be classified as “compliant”. Internal company rules and processes serve to control the behaviour of employees and to provide instructions and orientation for certain situations. They also have an organisational function in that they provide a framework for functions, tasks, duties and processes to protect the company and all acting persons and management levels from personal liability and legal risks. This framework is also determined by the formulation of principles, such as separation of functions, approval procedures and independent cross-checks (the principle of two-way or three-way review).

B. KEY CODES OF CONDUCT IN THE MEDICAL DEVICE INDUSTRY

In addition to the Medical Devices Code, the most important regulations in the medical device industry include guidelines for cooperation with health care facilities and health care professionals. These guidelines aim not only to avoid corruption risks, but also those risks that may arise in connection with medical device, competition, advertising, professional and social law. An example of the subject index of a typical bundling of the guidelines and regulatory areas under consideration in a manual (“Healthcare Compliance Professionals Manual”) is included in the [Subject Index Annex](#).

C. ORGANISATION-RELATED REGULATIONS AND PROCESSES

In the medical device industry, medical-scientific departments should routinely be organisationally separated from sales and marketing functions. Processes should also routinely be provided to ensure fair cooperation with medical professionals. Organisational rules and processes can be considered to achieve this goal. The terminology for such organisationally regulating measures varies widely. The terms include guidelines, manuals, work instructions, recommendations, etc., but also policies, guidelines, manuals, standards or SOPs (“Standard Operating Procedures”).

A clear organisational structure and process organisation requires a policy management system that clearly defines, among other things, which sets of rules and processes are used in the company, how they are to be designated and documented, what their hierarchy looks like and by whom they may be introduced, changed or revoked. It is crucial that all rules and processes (including IT-based processes) be effectively implemented so that they are legally binding for the employees. The rules and processes required for their area of work must be made available to employees in an up-to-date and orderly manner. The participation of the compliance officers in the form of approval requirements, veto rights or the like must be provided for when establishing or amending compliance-relevant rules and business processes. It must also always be considered that employee representatives can always have co-determination rights if rules and business processes influence the organisational behaviour of employees.

D. REQUIREMENTS SPECIFICATION: WHAT WILL AN AUDITOR ESSENTIALLY WANT TO KNOW?

- i. What behavioural and organisational rules and regulations exist in the company?
- ii. Is it defined how the rules and regulations are to be designated and documented, what their hierarchy is and by whom they may be introduced, changed or revoked?
- iii. How are rules and processes (including IT-based processes) implemented so that they are legally binding? Have any required co-determination rights of employees been considered?
- iv. How and where are the rules and processes required for their area of work made available to employees in an up-to-date and orderly manner?
- v. Is the involvement of the compliance functions in the definition or amendment of compliance-relevant regulations and business processes regulated and how are these structured?



Without a proper understanding of the rules, compliance cannot be expected

6. Training

A. KEY TO ENABLING COMPLIANT BEHAVIOUR

An essential factor for the efficiency of a compliance management system is the training of all employees at all levels. Without knowledge of the content of regulations and compliance-relevant contexts, compliance with and acceptance of the relevant rules cannot be expected.

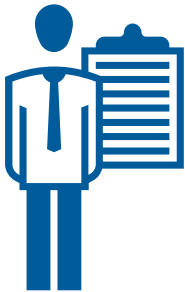
B. OCCASION AND METHOD

Training should be conducted regularly to refresh or deepen knowledge and as needed. A need for training may arise, among other things, in the case of new employees or in the case of changes with which existing employees need to be familiarised, such as changes in the law, new scientific or technical standards, etc., or new internal processes, restructuring, promotions, transfers, etc.. The training method should be based on the nature and scope of the training content and may require face-to-face training. E-learning or information letters may also be sufficient.

Managers should also regularly participate in face-to-face training. The company should develop criteria for identifying training needs and the applicable training method. An example of the contents of a training policy is included in the [Training Annex](#).

C. TRAINERS, QUALITY AND AUTHORITY

Training is to be prepared and delivered through internal or external training opportunities. The trainers should have the necessary technical competence as well as teaching skills and should be close to the relevant business environment to promote acceptance among the employees. If suitable external training is not used anyway to avoid considerable training costs, the quality requirements for training must be clearly defined in advance. This applies in particular to (maximum) duration, language, comprehensibility, practical relevance and knowledge tests. It must also be ensured that all training courses and the identity of participants are documented. Authority and accountability need to be established to ensure that training is provided on a regular basis and when specifically required, and by appropriate trainers using an appropriate training method.



D. REQUIREMENTS SPECIFICATION: WHAT WILL AN AUDITOR ESSENTIALLY WANT TO KNOW?

- i. Is training provided on a mandatory basis at regular intervals? Is it determined how training needs are to be identified?
- ii. Who is responsible for ensuring that employees receive training on a regular basis and when specifically required by appropriate trainers using an appropriate training method?
- iii. What document specifies the quality requirements for training and how are the quality requirements for conducted trainings to be documented?

E. TRAINING OFFERED FOR COMPLIANCE OFFICERS/MANAGERS BY THE BV MED ACADEMY

The BV Med Academy offers training courses for certified compliance managers. The event is aimed at employees of compliance or legal departments, managers from medical technology companies and medical institutions, as well as lawyers who want to focus more on this area professionally. During the event, the legal principles of compliance and extensive specialist knowledge will be conveyed. The training is specifically tailored to the area of the medical device industry, but teaches all compliance topics across the board.

It is based on the fundamentals of this BV Med Compliance Standard, the codes relevant to the medical device industry and is designed to be practical. Furthermore, the structure of a compliance management system, the analysis of risks in the company, effective control and the involvement and further training of employees are taught.

The quality of the compliance management system depends on its regular review

7. Compliance audits and self-reviews

A. IMPORTANCE OF REGULAR REVIEW AND IMPROVEMENT

The quality of the compliance management system and its effectiveness depend to a large extent on its regular review and improvement. Regular compliance audits are therefore an important part of the compliance organisation. Compliance audits are usually self-reviews by the company's own employees. At certain intervals, it may be advisable to commission an external body to conduct a compliance audit, especially if a neutral perspective and assessment appears necessary or useful.

Within the framework of compliance audits, it can be examined on the one hand whether the compliance management system meets the necessary requirements as they are essentially laid down in this BVMed Compliance Standard (system audit). On the other hand, the audit can examine whether the compliance management system is effective, i.e. whether all employees have actually complied with all requirements and rules, i.e. whether they were compliant (effectiveness audit).

Part B of this BVMed Compliance Standard presents benchmarks and criteria for a systematic self-review in the form of an internal compliance system audit.

B. WHO PERFORMS COMPLIANCE AUDITS?

The Compliance Department or the Compliance Officer have the right to conduct or initiate regular and ad hoc audits on compliance-relevant issues. In these investigations, they are free to choose the means and methods as well as the investigating bodies or departments. Accordingly, they can also involve or commission the internal audit and legal departments. It is also possible to commission external bodies to conduct compliance audits.

C. RULES FOR COMPLIANCE AUDITS

The audit frequency (also called "audit intervals"), the occasions for compliance audits and the responsibility for the audit reports must be determined. The same applies to the question of who is responsible for reporting to the company management and the development of suggestions for improvement or correction as well as the final decision on measures to be taken.

D. REQUIREMENTS SPECIFICATION: WHAT WILL AN AUDITOR ESSENTIALLY WANT TO KNOW?



- i. Where are the rules laid down with regard to the authority to conduct compliance audits, their occasions and frequencies, and the preparation of reports?
- ii. Who prepares recommendations for improvement resulting from identified complaints and who decides what action is taken?
- iii. To whom are the results of compliance audits reported?

8. Corrective measures and continuous improvement

A. OCCASIONS

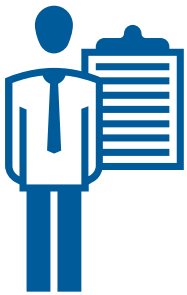
In the event of compliance violations, the compliance organisation will be reviewed to determine whether there is cause for corrective measures to prevent future compliance violations of similar content if possible. If a need for corrective measures is identified, it will be initiated immediately. The need for corrective measures may also arise from the results of a compliance audit or compliance risk assessment, as well as from changes in legal requirements or relevant industry codes. Improvement measures may be considered in particular if compliance indicators or the further development of generally accepted benchmarks suggest this.

B. RESPONSIBILITY

The compliance department or the compliance officers have the duty to continuously monitor the compliance management system for its suitability and effectiveness and to develop proposals for necessary and appropriate corrective measures or useful improvements. If the compliance functions cannot take corrective measures within the scope of their own competence, they must turn to the competent bodies.

C. REQUIREMENTS SPECIFICATION: WHAT WILL AN AUDITOR ESSENTIALLY WANT TO KNOW?

- i. Where is the duty to continuously monitor the compliance management system with regard to its suitability and effectiveness set out?
- ii. Who has authority for developing proposals for necessary and appropriate corrective actions or useful improvements?
- iii. Where are the occasions for taking corrective measures defined?



*Zero-tolerance
for
misconduct*

9. Internal investigations and sanctions

A. IMPORTANCE

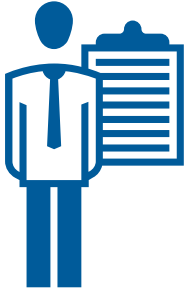
It is of paramount importance for the credibility of a company and the exemplary character of its management bodies and management teams (“tone from the top”) as well as for the seriousness of the values and compliance efforts it pursues that compliance-relevant misconduct is not tolerated in any way. For this reason, compliance violations must be determined through internal investigations within the framework of the possibilities legally available to a company. Depending on the results of the investigation, it may be necessary for compliance violations to have visible personal consequences for the employee concerned under certain circumstances. Insufficient participation of employees in compliance training or other compliance-related measures should also be decisively countered. Internal investigations are also important because a serious contribution to the clarification of compliance violations can have a penalty/fine-reducing effect in favour of the company.

B. RULES FOR INTERNAL INVESTIGATIONS

The compliance functions must ensure that sufficient suspicions of the existence of a compliance violation are looked into and that suspected cases are investigated and clarified. In these investigations, they are free to choose legally permissible means and methods (e.g. interviews, review of documents, files and business email correspondence, inspections). They also have the right to involve or commission other bodies or departments. The rules for conducting internal investigations should be set out in writing.

C. AUTHORITY TO IMPLEMENT SANCTIONS AND APPROPRIATENESS OF SANCTIONS

In the event of compliance violations, appropriate disciplinary measures are to be taken or initiated by the respective competent management. The appropriateness will be determined by the seriousness of the breach and the extent of its adverse impact on the company and its reputation. Accordingly, the measures to be taken may range from an admonition to a warning to termination. Compliance officers must be given the opportunity to comment on intended measures.



D. REQUIREMENTS SPECIFICATION: WHAT WILL AN AUDITOR ESSENTIALLY WANT TO KNOW?

- i. Has the company set out in writing the rules for conducting internal investigations?
- ii. In which document has the company regulated the duty to take appropriate sanctions in case of compliance violations?
- iii. Does the company make clear through notices or other announcements that compliance violations will result in mandatory sanctions?
- iv. Are the compliance functions involved in the procedure for imposing sanctions?

10. Documentation of the compliance organisation and its modules

A. SPECIAL IMPORTANCE

The documentation of the compliance organisation is of special importance. It provides the company and its employees with a clear overview of responsibilities, processes and competences. Furthermore, it also serves the purpose of proving to third parties that the company has an adequate compliance organisation and hence a preventive system that has been set up to prevent or significantly impede violations of the law. Only a coherent description of the compliance organisation allows third parties, be they regulatory bodies, investigative authorities or stakeholders in the health care and business sectors, to gain a quick and reliable impression of the compliance measures taken by the company.

B. WHAT SHOULD BE DOCUMENTED?

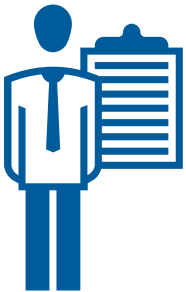
The description should reflect the company's basic understanding of compliance, for example with reference to the code of conduct or similar basic documents of the company, **see page 6 under point 1. B**. Furthermore, the cornerstones of the entire compliance management system are to be presented, i.e. the main compliance responsibilities with their tasks and competences, the whistleblower system and the supporting principles as described in the modules of this BVMed Compliance Standard.

Furthermore, the company must specify that compliance-relevant organisational measures, procedures and processes are to be documented. The same applies with regard to verification documents for compliance risk assessments, compliance audits, compliance training and other essential processes with compliance relevance.

C. WHERE SHOULD IT BE DOCUMENTED?

It is helpful for the description of the compliance management system and the individual modules of the compliance organisation to be made in the document that at the same time effects the legally binding establishment of the compliance organisation. This can be a policy, guideline or a similar legally binding document, depending on which organisation-related sets of rules are used in the company. The **Annex** contains the structure of a compliance organisation guideline with exemplary excerpts of individual sections.

D. REQUIREMENTS SPECIFICATION: WHAT WILL THE AUDITOR ESSENTIALLY WANT TO KNOW?



- i. In which document is the company's compliance management system presented with the essential elements of the compliance organisation?
- ii. Does the document provide a third party with a quick understanding of the compliance management system and its key organisational elements?
- iii. Has the company determined that compliance-relevant organisational measures, procedures and processes are to be documented, as well as other essential processes with compliance relevance?

*Systematic
review of the
compliance
organisation
using
benchmarks and
industry
practice*

B. Self-audit of the compliance organisation

1. Subject of the self-review
2. Procedure of the System Audit
3. Benchmarks for the System Audit
4. Audit report

1. Subject of the self-review

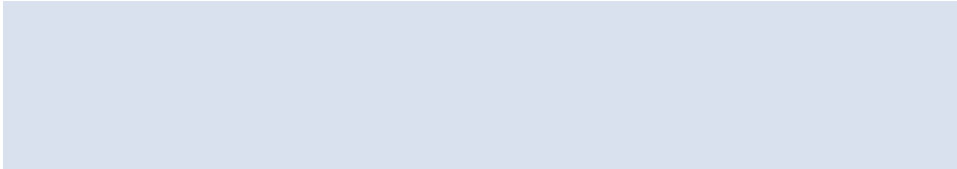
Standards and criteria for a systematic self-review in the form of an internal compliance system audit are presented below.

The internal compliance system audit according to this section (hereinafter referred to as “System Audit”) is intended to allow the company to make a statement as to whether it can be proven on the basis of its documentation that the organisational measures of the individual modules provided for in this BVMed Compliance Standard have been taken. Accordingly, the System Audit does not aim to determine whether the measures taken by the company have been implemented in a legally binding and effective manner or whether they are actually followed and lived in company practice. Rather, the System Audit serves in a formal procedure according to this section to systematically check whether the company’s compliance organisation corresponds to today’s customary and generally recognised benchmarks and industry usages.

2. Procedure of the System Audit

The initiation of a System Audit requires a written mandate from the management to a suitable auditor. If possible, this auditor should not belong to the company’s compliance officers to avoid conflicts of interest. In this respect, an employee from the internal audit or controlling departments could be considered. It could make sense for such a review to be supported by an internal or external specialist who has experience in assessing compliance management systems. In view of the goal of providing the greatest possible legal relief from liability to protect the company, its employees and management levels, assistance from a lawyer is the main option. A self-review of the compliance management system can also be performed by the compliance officers at any time outside the regulations for a System Audit according to this section, namely within the scope of their regular compliance audit authorisation (**see module A.7.**). In practice, it will be advisable for compliance officers to conduct a pre-audit prior to a System Audit to prepare for the System Audit to be conducted by the auditor and to identify weaknesses in advance that can then be remedied prior to the System Audit.

In the mandate to the auditor, it must be stated that the System Audit consists of an examination of the documentation for the implementation of the individual modules of the BVMed Compliance Standard as well as the measures and management processes taken. The audit concerns the company designated in the mandate.



The mandate will certify to the auditor that the company in question is to provide him with all appropriate documents for the performance of the System Audit and that he is to be granted access to independent or geographically separate branches and subsidiaries on request.

The auditor will also be authorised, in addition to assessing these documents within the scope of his dutiful discretion, to evaluate the documents provided in more detail by means of interviews and discussions with managers and other employees of the company on site.

The order will specify the date of commencement and the duration of the System Audit.

The System Audit is completed when the audit report is sent to the management. In practice, the management, the auditor, the compliance officers and, if applicable, the external consultant routinely agree on which conclusions are to be drawn from the System Audit and which additional measures are to be initiated by when and with a budget to be determined.

3. Benchmarks for the System Audit

The benchmark for the audit of the company's compliance management system is the requirements of the BVMed Compliance Standard.

The company's compliance management system fulfils the requirements of the BVMed Compliance Standard even if individual requirements of the BVMed Compliance Standard are not fully fulfilled, but in the opinion of the auditor, these missing points are of minor importance in the overall assessment of the company's compliance management system with regard to the type and scope of the company's business activities.

The audit is basically at the discretion of the auditor, who must determine his own methodological procedure, factoring in the BVMed Compliance Standard.

The scope of the System Audit usually depends on the legal form, the size and the organisational structure of the company to be audited. The standard of orientation for the audit questions to be asked is the specification of the respective module of the BVMed Compliance Standard.

4. Audit report

The auditor will prepare a detailed report on the performance of the System Audit.

The report will also contain the auditor's summary statement as to whether the audited company has established a compliance management system in accordance with the requirements of the BVMed Compliance Standard, i.e. whether the organisational measures of the individual modules have been taken according to the documents provided.

The auditor's report should be based in its presentation and structure on the questions in the specifications of the respective module of the BVMed Compliance Standard and in each case make clear reference to the documents provided to answer the questions. If the auditor does not consider individual requirements of the BVMed Compliance Standard to be fully met, he must give detailed reasons as to whether, in his opinion, the missing points are of material or minor importance in the overall assessment of the company's compliance management system.

*Concentration
on the essential
elements of an
appropriate
compliance
organisation*

Concluding note

This BVMed Compliance Standard is limited to the essential elements of an appropriate compliance organisation and their practical implementation in companies of the medical device industry. Further criteria and elements can be found in the following standards and publications:

- > ISO 37301 Compliance Management Systems – Requirements with guidance for use
- > ISO 37001 Anti-bribery Management Systems – Requirements with guidance for use
- > TÜV Compliance Management Systems – Standard and Guideline TR CMS 101:2015 and TR CMS 100:2015
- > Corporate Responsibility and Corporate Compliance: A Resource for Health Care Boards of Directors, published by the Office of Inspector General (OIG) of the U.S. Department of Health and Human Services and the American Health Lawyers Association (AHLA), available at <http://oig.hhs.gov/compliance/compliance-guidance/docs/Practical-Guidance-for-Health-Care-Boards-on-Compliance-Oversight.pdf>
- > Seven fundamental elements of an effective compliance program, published by the Office of Inspector General (OIG) of the U.S. Department of Health and Human Services.



BVMed - Bundesverband Medizintechnologie e. V.
Reinhardtstr. 29 b, 10117 Berlin
Tel.: +49 (0)30 246 255-0