TR CMS 101:2011

Standard for Compliance Management Systems (CMS)

of TÜV Rheinland, Cologne

TÜVRheinland®
Precisely Right.

Total scope: 22 pages

TÜVRheinland®
Precisely Right.

Contents

Foreword ..... - 3 -
0 Introduction ..... - 5 -
1 Field of application ..... - 5 -
2 Aims of the compliance management system ..... - 6 -
3 Terms ..... - 6 -
4 Compliance management system ..... - 7 -
4.1 General requirements ..... - 7 -
4.2 Documentation requirements ..... - 8 -
4.2.1 General ..... - 8 -
4.2.2 Control of specifications ..... - 9 -
4.2.3 Control of records ..... - 10 -
5 Responsibility of the management ..... - 10 -
5.1 Obligation of the management ..... - 10 -
5.2 Responsibility, authority and communication ..... - 11 -
5.2.1 Responsibility and authority ..... - 11 -
5.2.2 Compliance Officer ..... - 11 -
5.2.3 Internal communication ..... - 12 -
5.3 Management evaluation ..... - 12 -
5.3.1 General ..... - 12 -
5.3.2 Input for the evaluation ..... - 13 -
5.3.3 Results of the evaluation ..... - 13 -
6 Management of resources ..... - 14 -
6.1 Provision of resources ..... - 14 -
6.2 Personnel resources ..... - 14 -
6.2.1 General ..... - 14 -
6.2.2 Expertise, training and awareness ..... - 14 -
6.3 Infrastructure ..... - 15 -
7 Compliance processes and implementation ..... - 15 -
7.1 Specific compliance risks affecting the organisation ..... - 15 -
7.2 Applicable compliance requirements ..... - 15 -
7.3 Decision on the appropriate measures to fulfil the compliance requirements - 16 -
7.4 Integration of the compliance requirements in the work processes ..... - 16 -
7.5 Dealing with compliance-relevant conflicts of interest ..... - 16 -
7.6 System of clearances, approvals and authorisations ..... - 16 -
7.7 Whistleblower system ..... - 17 -
7.8 Advice, support ..... - 17 -
7.9 Dealing with compliance-relevant processes ..... - 17 -
7.10 External service providers ..... - 18 -
8 System monitoring, analysis and improvement ..... - 18 -
8.1 Internal audits ..... - 18 -
8.2 Monitoring ..... - 19 -
8.3 Improvement ..... - 19 -
8.3.1 Constant improvement ..... - 19 -
8.3.2 Corrective measures ..... - 20 -
8.3.3 Preventative measures ..... - 20 -
References ..... - 22 -

Foreword

Top management are responsible for the installation, maintenance and constant improvement of a management system to fulfil the compliance requirements. As a cross-cutting issue, compliance affects all areas and functions within an organisation. Compliance measures are not implemented on an isolated basis but must be integrated in the organisation's administrative and operational processes. This requires a systematic approach to achieve fulfilment of the compliance requirements throughout the organisation.

In view of the significance of compliance and the possible consequences of breaches of compliance requirements, the compliance management system is an independent management system. The compliance management system features points of contact with other management systems and rules and regulations (e.g. corporate governance, risk management, quality management, environmental management, business continuity management, sustainability management).
Compliance requirements are not static but are subject to frequent changes (e.g. because of changes to legislation, the acceptance of new activities or the extension of activities to new regions). To bring the compliance management to fruition and to improve it constantly, an iterative process is required, which is presented in the following overview:

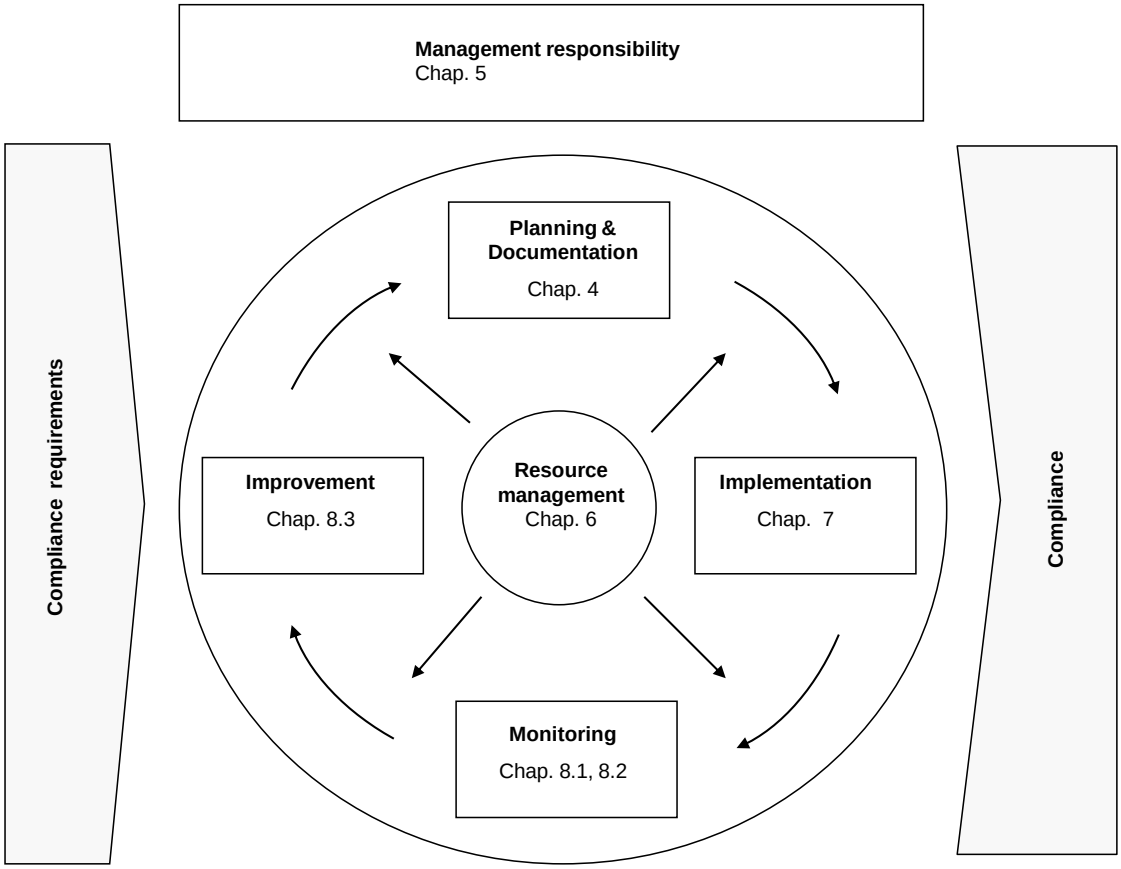

Figure 1- Model of a process-based Compliance Management Systems (CMS) ©

The documentation of the compliance management system allows it to be implemented and maintained independently.

The effective implementation and maintenance of a compliance management system and its communication within the organisation and externally also generates additional opportunities for the organisation. The confidence this engenders in stakeholders (e.g. employees, customers, authorities, shareholders, investors) can result in more sustainable relationships (e.g. greater customer loyalty, long-term business relationships, greater motivation among employees). The organisation can also benefit from lower costs for corrective measures, more favourable financing terms and insurance premiums.

0 Introduction

This standard highlights the basic elements, which a management system must contain to fulfil the compliance requirements applicable for the organisation; the specific structure and implementation of the compliance management system depend on the organisation and are the responsibility of top management.

The elements of the compliance management system highlighted in this standard are testable and detectable, to establish whether and in which respects an organisation has a compliance management system that fulfils the targets described in section 2. Compliance management systems may be differently structured or documented in a way that is specific to the organisation.

The TR CMS 101:2011 standard for compliance management systems allows an organisation to be issued with a certificate, having successfully carried out the system audit, confirming that it demonstrably

a) maintains an effective compliance management system,

b) fulfils the minimum requirements of a compliance management system, and

c) is in a position to implement preventative and corrective measures.

Certification of the compliance management system does not constitute a statement that the organisation actually fulfils all applicable compliance requirements; the execution of the certification audit does not represent advice with regard to the applicable rules or legal advice. A certification audit or certification does not, in principle, relieve the organisation from liability in the case of corporate negligence or breaches of its duty of supervision. Specifications for the audit and test instructions are set down in a separate guideline by TÜV Rheinland.

1 Field of application

The present standard stipulates the fundamental elements that are part of a compliance management system. It is applicable to all organisations both at home and abroad.

The structure and realisation of the compliance management system are influenced by

a) the size and structure of the organisation, the nature of its activities,

b) the regions in which the organisation operates,

c) the products produced,

d) the processes applied,

e) the environment, changing requirements,

f) specific risks affecting the organisation and

g) the organisation's particular aims.

Elements of the compliance management system must be stipulated in such a way that they can be detected and tested. This allows the fact of whether the organisation has an effective compliance management system to be determined.

2 Aims of the compliance management system

The aim of the compliance management system is systematically to create the preconditions in the organisation that will ensure breaches of compliance requirements are avoided or made significantly more difficult and breaches that have occurred can be recognised and dealt with.

3 Terms

Outsourced compliance processes	Compliance-relevant processes, which are carried out by an external office on the basis of a decision by the organisation.
Audit	Audit
Business continuity management	Ensuring the maintenance of key processes in an organisation following the occurrence of serious events
Compliance	Fulfilment of compliance requirements (please refer to that section)
Compliance requirements	All rules and regulations, which must be observed by the organisation and the people working there, irrespective of whether these are statutory or official compliance requirements or requirements that have been imposed on the organisation by itself or imposed by another organisation on its staff.

Compliance Officer	Member of top management tasked with implementing the elements of the compliance management system
Compliance culture	Internal acceptance of compliance requirements, behaviour that reflects them and actual consideration of compliance requirements in the organisation
Whistleblower System	Option of being able to turn to an (internal or external) contact point with compliance-relevant information outside the normal reporting channels
Key figures in measuring compliance	Measurable statistics, which allow numerical conclusions to be drawn regarding the effectiveness of the compliance management system (e.g. number of breaches of compliance requirements recognised)

4 Compliance management system

4.1 General requirements

The organisation must introduce a compliance management system, document it, realise it, maintain it and constantly improve its effectiveness.

The organisation must

a) stipulate the processes required for the compliance management system and its application throughout the organisation,

b) stipulate the sequence and interaction of these processes,

c) stipulate the criteria and methods required to ensure that these processes are executed and controlled effectively,

d) ensure that the resources and information needed to execute and monitor these processes are available,

e) monitor these processes, measure and analyse them, if appropriate, and

f) take the measures needed to achieve the planned results and a constant improvement in these processes.

The organisation must guide and control these processes in compliance with the requirements of this standard.

If the organisation decides to outsource compliance-relevant processes, it must ensure that processes of this kind are controlled. The scope and extent to which outsourced processes of this kind are controlled must be stipulated in the compliance management system.

NOTE The outsourcing of compliance-relevant processes does not relieve the organisation of the duty to fulfil the compliance requirements applicable to it.

4.2 Documentation requirements

4.2.1 General

The documentation on the compliance management system must contain the necessary specifications and records.

The usual specifications are:

a) Legal sources; including laws, ordnances, administrative acts, articles of association, binding standards or codes,

b) List of specific compliance requirements applicable to the organisation (manuals, guidelines),

c) Description of the compliance management system,

d) Documented procedures and processes or operating instructions to ensure fulfilment of compliance requirements and to network compliance-relevant processes with other processes and

e) Documented procedures, which are required by this standard.

The usual records are:

a) Records of results of compliance audits and corrective measures,

b) Compliance reports,

c) Risk analyses and evaluations

d) Records of key figures in measuring compliance,

e) Minutes of top management's involvement with compliance issues

f) Documents on the conduct of compliance training sessions,

g) Documents on breaches of compliance requirements and the measures and sanctions adopted in these cases,

h) Records, which the organisation has classified as necessary to ensure the effective planning, execution and control of its processes, and

i) Records prescribed by law.

4.2.2 Control of specifications

The specifications required by the compliance management system must be controlled. A documented procedure to stipulate the requisite control measures must be introduced to

a) approve documents before they are issued,

b) evaluate documents at planned intervals, to update them if necessary and to approve them once more,

c) ensure that amendments and the current revision status of documents are marked,

d) ensure that the valid versions of relevant documents are available at the respective locations,

e) ensure that documents are legible and comprehensible for those affected,

g) prevent the unintended use of out of date documents and to mark these appropriately if they are stored,

h) ensure that statutory posting and display duties are complied with and

i) ensure that documents and records are stored and protected in a suitable manner for the duration of the

storage period imposed by law or otherwise, that they are legible, easily recognisable and are easily retrievable.

4.2.3 Control of records

Records of compliance with compliance requirements must be controlled.

The organisation must introduce a documented procedure to stipulate the control measures, which are required for the marking, storage, protection, retrievability of records, compliance with the storage period and the availability of records.

Records must be legible, easily recognisable and stored in a way that makes them retrievable.

5 Responsibility of the management

5.1 Obligation of the management

Top management must demonstrate the development and realisation of the compliance management system and the constant improvement of its effectiveness by

a) conveying the binding force of compliance requirements and the significance of compliance with compliance requirements to the organisation,

b) giving a commitment to the creation of a compliance culture, in particular, expressing its expectation that compliance requirements will actually be complied with,

c) aligning the organisation’s aims and values with the compliance requirements,

d) reviewing the compliance risk analysis with regard to actual risks on a regular basis and adjusting it, if applicable,

d) carrying out management evaluations of the compliance management system on a scheduled basis,

e) ensuring that resources are available and

f) monitoring the ongoing appropriateness and functioning of the compliance management system.

5.2 Responsibility, authority and communication

5.2.1 Responsibility and authority

Top management must ensure that responsibilities and authorities are stipulated and disclosed within the organisation.

5.2.2 Compliance Officer

Top management must carefully select and appoint a member of the organisation's management, who will have the responsibility and authority, alone or in cooperation with others:

a) to work towards the processes required for the compliance management system being introduced, realised and maintained,

b) to report to top management on the performance and effectiveness of the compliance management system and any need for improvements,

c) to ensure awareness and communication of compliance requirements through the organisation and

d) to pick up compliance-relevant events on his own initiative, to document them and report them to top management.

Top management will allow the Compliance Officer to perform his compliance tasks independently. It will not assign any additional tasks to the Compliance Officer, which could entail conflicts of objectives with fulfilment of the compliance tasks.

5.2.3 Internal communication

Top management must ensure that suitable communication processes are introduced and maintained within the organisation as a whole and communication takes place with regard to the effectiveness of the compliance management system. Communication must include informing everybody of the compliance requirements affecting them and

drawing attention to possible consequences of compliance breaches. Top management must ensure that recognised breaches of compliance requirements are reported without delay.

Top management must ensure that it complies with its duties to provide information and report on compliance issues to the internal supervisory bodies. The internal supervisory bodies are involved with the organisation's compliance issues in accordance with their statutory supervisory duties and duties of care.

5.3 Management evaluation

5.3.1 General

Top management must evaluate the organisation's compliance management system at appropriate intervals on a scheduled basis to ensure its ongoing suitability, appropriateness and effectiveness. The evaluation must include the evaluation of options for improvements and the need for amendments regarding the compliance management system.

Records of the management evaluation must be maintained.

5.3.2 Input for the evaluation

Input for the management evaluation must contain information on the following:

a) Results of audits,

b) References to compliance-relevant issues from employees, business partners, customers, users, authorities, associations etc.,

c) Reports of recognised breaches of compliance requirements,

d) Status and effectiveness of preventative and corrective measures and expenditure for corrective measures taken,

e) Follow-up measures to previous management evaluations and results of follow-up measures of previous monitoring,

f) Changes, which could have an impact on the compliance management system (e.g. legal changes, changes in the risk situation),

g) Recommendations for improvements and

h) Key figures in measuring compliance.

5.3.3 Results of the evaluation

The results of the management evaluation must contain decisions and measures on the following:

a) Improvement of the effectiveness of the compliance management system and its processes,

b) Demand for resources and

c) Covering the identified demand for training on compliance-relevant processes

6 Management of resources

6.1 Provision of resources

The organisation must identify and provide the resources needed to realise the compliance management system, to maintain it and to improve its effectiveness constantly.

6.2 Personnel resources

6.2.1 General

People, who have to observe compliance requirements for their work, must have the education, training, skills and experience needed to fulfil these requirements.

6.2.2 Expertise, training and awareness

The organisation must

a) systematically identify and evaluate the training demand needed to achieve the requisite expertise to fulfil the compliance requirements,

b) carry out the compliance training or other measures needed to convey this expertise.

c) assess the effectiveness of the measures taken,

d) generate understanding of the significance of fulfilling compliance requirements and awareness of the possible consequences of compliance breaches and

e) maintain suitable records of education, training, expertise and experience as well as other measures to promote the requisite expertise.

6.3 Infrastructure

The organisation must identify, provide and maintain the infrastructure needed to fulfil the compliance requirements.

If required, the organisation must allow access to (internal or external) legal advice with regard to the extent, the applicability, the validity and the reach of compliance requirements.

7 Compliance processes and implementation

7.1 Specific compliance risks affecting the organisation

The organisation must systematically analyse and identify compliance risks, which result from its size, structure, the nature of its activity and the regions in which it operates.

Top management must

a) ensure that it receives regular reports on the organisation's compliance risks, and

b) regularly evaluate the organisation’s specific compliance risks and take suitable measures to prevent them.

7.2 Applicable compliance requirements

The organisation must

a) systematically analyse and identify the compliance risks specifically applicable to it because of its activities (e.g. services, products, geographical regions) and document the procedure for this purpose,

b) monitor amendments to the specifically applicable compliance requirements and the impact of these amendments on the organisation on an ongoing basis,

c) decide on the introduction of mandatory compliance specifications, which do not already apply by law or official decree,

d) document the compliance requirements specifically applicable to it and make them available and

e) ensure that all those affected are informed of the applicable compliance requirements and

f) update the documentation of the compliance requirements specifically applicable to it on an ongoing basis.

7.3 Decision on the appropriate measures to fulfil the compliance requirements

The organisation must have processes, with which it can ensure that the appropriate measures to fulfil the compliance requirements are taken and the appropriate processes for the size and structure of the organisation, the nature of its activity and the regions in which it operates are introduced.

7.4 Integration of the compliance requirements in the work processes

Work processes must be structured in such a way that fulfilment of the compliance requirements is facilitated and made possible.

7.5 Dealing with compliance-relevant conflicts of interest

The organisation must have processes with which possible and actual compliance-relevant conflicts of interest can be identified.

It must provide those affected by requirements with criteria as to how they must deal with possible and actual compliance-relevant conflicts of interest. This is also true with respect to conflicts between the interests of the organisation on the one hand and the interests of customers or users on the other.

The organisation must ensure that there is the appropriate separation of functions needed to avoid compliance-relevant conflicts of interest.

7.6 System of clearances, approvals and authorisations

The organisation must have a system of authorisations for clearances and approvals that is suitable to avoid breaches of compliance requirements.

The valid clearance thresholds, approval requirements and the necessity of several persons working together to execute compliance-relevant transactions must be documented and disclosed within the organisation.

7.7 Whistleblower system

The organisation must establish an (internal or external) contact point and publicise it within the organisation, which will allow people to provide

compliance-relevant information (e.g. on recognised breaches of compliance requirements) - anonymously, if required - or contribute suggestions.

The processes in dealing with compliance-relevant information and suggestions received by the contact point must be documented. Whistleblowers will receive feedback on the treatment of their information and suggestions unless they are anonymous.

NOTE A new function does not necessarily have to be created for the whistleblower system. However, the whistleblower system must allow people to turn to a contact point with compliance-relevant information outside the organisation's normal reporting channels

7.8 Advice, support

The organisation must ensure that those affected receive advice and support if they have questions on compliance-relevant issues and in dealing with conflicts of interest.

7.9 Dealing with compliance-relevant processes

The organisation must have a documented procedure for dealing with compliance-relevant transactions, including responsibilities and reporting channels.

The organisation must ensure that the external communication prescribed by law (e.g. duties to report, notify, provide information and warnings vis-à-vis the authorities) is possible.

All relevant compliance transactions, as well as their treatment and solution, must be documented.

7.10 External service providers

The organisation must ensure that at least the same compliance requirements apply to external service providers, which it makes use of to fulfil its compliance requirements or which it involves in compliance relevant transactions, as to the organisation itself.

8 System monitoring, analysis and improvement

The organisation must plan and realise the monitoring, analysis and improvement processes needed to ensure the effectiveness of the compliance management system.

8.1 Internal audits

The organisation must carry out internal audits at planned intervals to establish whether the compliance management system

a) fulfils the compliance requirements and the requirements for the compliance management system described in this standard and

b) is effectively realised and maintained.

An audit programme must be planned under which the status and the significance of the processes and areas as well as the results of previous audits must be taken into account. The audit criteria, the audit scope, the audit frequency and the audit methods must be stipulated. The choice of audits and the execution of the audit must ensure the objectivity and impartiality of the audit process. Auditors may not audit their own work.

The organisation will decide on the responsibilities and on the execution of audits as well as on the reporting of the results and on the maintenance of records. The key results of the compliance audit must be reported to top management.

Records of audits and their results must be maintained.

The management responsible for the audited area must ensure that any corrections and corrective measures required must be taken to rectify recognised deviations and their causes without unjustified delay. Follow-up measures must include verification of the measures taken and reporting on the results of the verification.

8.2 Monitoring

The organisation must use suitable methods to monitor the compliance management system and document the results of monitoring the compliance management system. These methods must show that the processes introduced are capable of fulfilling the compliance requirements.

Monitoring must refer to the compliance-relevant processes outsourced by the organisation and the external offices used to execute these processes.

Where applicable, key figures in measuring compliance must be introduced and used to establish the effectiveness of the processes to fulfil the compliance requirements.

Notifications or reports on compliance-relevant incidents or events (including breaches of compliance requirements) received will be picked up immediately and on a scheduled basis and reported to the defined offices.

If the planned results are not achieved, corrections and corrective measures must be taken, if appropriate.

The status of corrective measures must be followed up on an ongoing basis by the persons responsible specified by the organisation.

8.3 Improvement

8.3.1 Constant improvement

The organisation must constantly improve the effectiveness of the compliance management system on the basis of the results of the monitoring including the audit results, the compliance key figures and the management evaluations.

8.3.2 Corrective measures

The organisation must take appropriate corrective measures to rectify the causes of recognised breaches of compliance requirements, in order to prevent their occurring again.

A documented procedure must be introduced to stipulate requirements for

a) the evaluation of breaches of compliance requirements,

b) the establishment of causes of breaches of compliance requirements,

c) the assessment of the need for action to prevent breaches of compliance requirements occurring again,

d) the establishment and realisation of the requisite measures,

e) recording the results of the measures taken,

f) assessing the effectiveness of the measures taken and

g) assessing the effectiveness of the monitoring measures.

8.3.3 Preventative measures

The organisation must stipulate appropriate measures for rectifying the causes of possible breaches of compliance requirements, to prevent their occurring.

A documented procedure must be introduced to stipulate requirements for

a) the establishment of possible future breaches of compliance requirements and their causes,

b) the assessment of the need for action to prevent breaches of compliance requirements occurring,

c) the establishment and realisation of the requisite measures,

d) recording the results of the measures taken and

e) assessing the effectiveness of the preventative measures taken.

References

ISO 9001:2008

ONR 49001:2004

BS 25999

AS 3806-2006

ISO 26000:2010