**Prof. Dr. jur. Josef Scherer**

Lawyer and consultant, professor of compliance, risk and crisis management, restructuring and insolvency law, and head of the ESGRC department at Deggendorf Institute of Technology; former judge at the regional court.

***Scherer***

# The dangerously old new features of ISO 9001:2026

- **Liability-based obligation to appropriately integrate governance, risk, compliance, and process management into the quality management system (Part 1)**

  **Deggendorf, January 1, 2026**


This article is the first in a series that deals with the (old and new) requirements of the revised ISO 9001:2026 (quality management system) from a governance, risk, and compliance perspective and provides an overview of the topics that still need to be explored in greater depth.

The current plan of ISO and DIN is to publish the final version of ISO 9001:2026 in September 2026. This will be followed by a transition period for the change from ISO 9001:2015 to the new standard. As early as the last revision of ISO 9001 in 2015, *Scherer and Fruth*[1] showed that governance, risk, compliance (GRC), and *appropriate* process management are indispensable in quality management.

The GRC and process requirements now apply *to all management system standards.*

In the author's opinion, this has been frequently ignored for 10 years by QM and other management system officers, internal and external auditors, and certification bodies, without explicitly clarifying what was *not* considered in the specific application. In practice, this creates a system that is more for appearances and a dangerous sense of certainty. This should now come to an end. The new DIN ISO 9001 provides an opportunity to enhance the quality management system. Conversely, an interpretation of the standard that is free of risk and compliance would greatly reduce the value of a QM system. Without precautions, it would even be dangerous.

The new DIN ISO 9001 therefore offers many opportunities when applied critically and correctly, but also considerable risks when applied without reflection and without GRC expertise. The current transformation in all areas also requires a fundamental rethink in quality management.

## 1. Planned changes and impact on other standards

In 2026, ISO 14001 (environmental management system) will be revised alongside ISO 9001 (quality management system), and in 2027, ISO 45001 (occupational health and safety management) will be revised, each with a three-year transition period.

*The following information applies to all management system standards.*

The new ISO standard 9001:2026 (quality management system)[2] , expected in fall 2026, contains a number of changes that are more or less liable for organizations, managing directors, board members, QM officers, internal and external auditors, and certification bodies wishing to implement or certify.

This standard forms the basis for further industry-specific standards, meaning that the information provided in this article should also be considered (and as early as this articles publishing):

[1] See *Scherer, Fruth*, Danke, ISO! Über die neue ISO 9001:2015 (Qualitätsmanagementsystem) zum integrierten, ganzheitlichen Managementsystem mit Governance, Risk und Compliance (GRC), BCM - Berufsverband der Compliance Manager, Compliance 2015 - Perspektiven einer Entwicklung, Regensburg 2015, pp. 83–107, available for free download at: https://www.scherer-grc.net/files/fil/danke-iso.pdf.
[2] See DIN EN ISO 9001 Quality management systems – Requirements (ISO / DIS 9001:2025-9).

## Examples:

*Automotive industry*: IATF 16949, an international standard for quality management in the automotive supply industry, fully requires ISO 9001 and supplements it with industry-specific requirements.

*Automotive service & aftermarket (VDA 6.1)*: The VDA 6.x series, including VDA 6.1, forms an independent German QM standard for manufacturers and suppliers in the automotive industry, historically derived from ISO 9001, but now managed as an independent certification system.

*Aerospace*: EN 9100 / AS 9100 / JISQ 9100 are QM standards for the aerospace industry in Europe, the USA, and Japan. ISO 9001 forms the core, supplemented by strict safety and documentation requirements.

*Clinics*: EN 15224 is a European quality management standard for healthcare, based on ISO 9001, expanded to include specific requirements for clinical processes, patient-related risks, safety, and evidence-based care.

*Medical devices*: ISO 13485[3] is a standalone quality management standard for medical devices, based in part on ISO 9001, but with a much stronger regulatory focus and risk-based approach, with specific requirements for product safety, traceability, and regulatory compliance.

*Telecommunications/ICT*: TL 9000, a QM model for telecommunications and IT hardware/software, is based on ISO 9001 but includes additional measurement and performance metrics.

*Energy supply*: ISO 19443 regulates quality management for the nuclear supply chain and extends ISO 9001 to include safety and risk management.

*Educational services*: ISO 21001 (EOMS) is a QM system specifically for educational organizations.

*Oil, gas, and petrochemicals (API Q1 / Q2):* The API specifications Q1 and Q2 are independent QM standards of the American Petroleum Institute for production and service organizations in the oil and gas industry. They are based on quality management principles similar to ISO 9001 and supplement these with comprehensive risk-related, safety-relevant, and production-specific requirements.

*Railway industry:* ISO 22163 (IRIS) contains the QM standard for the railway sector, is structurally based on ISO 9001, and contains additional performance requirements.

*Authorities & public organizations*: ISO 18091 is the QM standard for local government, tailored to public services and based on ISO 9001.

The planned changes to ISO 9001 are not particularly spectacular, although numerous consultants, certifiers, and others who stand to profit from them may discover a considerable need for consulting services—at a cost:

***"Changes[4]***

*The following changes have been made compared to DIN EN ISO 9001:2015-11 and DIN EN ISO 9001/A1:2024-11:*

[3] ISO 13485:2016 was reconfirmed by ISO in November 2025 as remaining valid until 2030.
[4] See DIN EN ISO 9001 Quality management systems – Requirements (ISO / DIS 9001:2025-9)

*a) Current requirements of the "harmonized structure for management system standards" specified in the ISO directives have been incorporated and the corresponding content has been clarified and standardized in terms of language.*

*b) In this context, terms 3.1 to 3.20 from the harmonized structure for management system standards have been added to Section 3 (without changing the reference to DIN EN ISO 9000, Quality management systems — Fundamentals and vocabulary).*

*c) the contents of DIN EN ISO 9001/A1:2024-11 with additions relating to climate-related measures have been integrated;*

*d) comments on requirements have been checked for topicality and completeness and partially adapted;*

*e) Additional requirements and comments have been included in 5.1.1, 8.2, 8.3.1, 8.3.3, 8.5.1, 9.3.2, and 10.2.1, among others.*

*f ) 5.1.1 has been supplemented with requirement i) "Promotion of a culture of quality and ethical behavior";*

*g) In 5.2.1 on quality policy, requirement e) was added, according to which the context of the organization and strategic direction must be considered.*

*h) 6.1 "Measures for dealing with risks and opportunities" has been supplemented by 6.1.2 "Measures for dealing with risks" and 6.1.3 "Measures for dealing with opportunities";*

*i) Extended requirements are set out in 6.3 e), f), and g) for planning changes;*

*j) In 7.3 "Awareness," requirement e) "Quality culture of the organization and ethical behavior" has been added.*

*k) Informative Annex A "Explanation of structure, terminology, and concepts" has been fundamentally revised to aid understanding of the requirements. Changes to the previous version are no longer listed.*

*l) Informative Annex B "Other International Standards of ISO/TC 176 on Quality Management and Quality Management Systems" has been deleted without replacement.*

*m) The current German translation of the harmonized structure has been used and, in this context, the use of "lenken/Lenkung" (control/control) in relation to documented information has been replaced by "steuern/Steuerung" (steer/steering), and two new national footnotes N1 and N3 have been added.*

*n) Document editorially revised."*

The standard still has weaknesses and needs clarification; some new approaches are welcome.

*From a compliance perspective,* the requirements for a (quality) management system are already more demanding than presented at first glance in the current and revised version. There is indeed an urgent need for action here, even now:

## 2. Clarification of the legal nature of management system standards and the primacy of legally binding requirements: none

Since there are no legally prescribed definitions (legal definitions) for management systems, different names and terms are used, such as "management system.[5]

First, an attempt at a definition of "management system":

"*A management system consists of formally specified, ideally networked and interacting components, such as structural and procedural organization, resources, input and output, with the purpose of supporting an organization in setting objectives, planning, controlling and monitoring to achieve mandatory and optional goals*."[6]

Every "living" organization already has a management system per se. In every organization, something is happening. There is a structural and procedural organization, a control loop, often chaotic, undocumented, unconscious and sometimes quite passable or even considered as a "best practice."

ISO 9001 specifies "requirements" for quality management systems.

As with many other standards, the new QM-9001 standard initially lacks an explanation of the required nature of the creation and legal quality of a standard ("*anticipated expert* opinion") and a reference to the absolute priority of legally binding requirements.[7]

Nor does it specify whether this standard reflects the recognized state of science and practice, the recognized rules of technology, state of the art or the latest state of science and technology.[8]

## 3. Appropriate reference to compliance and liability of the executive bodies and QM officers: None

[5] See *Scherer*, Sustainable Management and Monitoring of Organizations (Governance) according to DIN ISO 37000, Successful Implementation, Auditing, and Reporting, published by DIN, DIN Media Verlag, 2025, Introduction chapter.
[6] See also DIN EN ISO 9001 Quality Management Systems – Requirements (ISO / DIS 9001:2025) and ISO 37301:2021 (Compliance Management Systems), which *describe* a management system as *a set of interrelated or mutually influencing elements that are used to define policies and objectives and achieve these objectives.*
[7] See *Scherer*, Sustainable Management and Monitoring of Organizations (Governance) according to DIN ISO 37000, Successful Implementation, Auditing, and Reporting, published by DIN, DIN Media Verlag, 2025, Chapter 1.
[8] See *Scherer, Fruth*, Technik-Governance (Technology Governance), special edition BCM-Berufsverband der Compliance Manager (BCM Professional Association of Compliance Managers), 2016, available for free download at: https://www.scherer-grc.net/files/fil/bcmtechnikgovernance.pdf, and *Scherer*, Sustainable Management and Monitoring of Organizations (Governance) according to DIN ISO 37000, Successful Implementation, Auditing, and Reporting, published by DIN, DIN Media Verlag, 2025, Introduction chapter.

### 3.1 Mandatory requirements according to the principle of legality

First, (management) systems, products, services, works, or other services[9] , processes, etc. must comply with mandatory obligations (laws/case law/recognized rules or state of the art[10] , etc.) (compliance-based approach and general obligation to act lawfully).[11]

### 3.2 References and mandatory requirements for compliance in the (new) ISO 9001

The draft of the revised ISO 9001 contains *requirements in many different places to identify, evaluate*, *and comply with legal requirements for products and services*, which corresponds to compliance management in relation to an organization's performance.

**A few examples of many (quotes from the text of the draft of the new DIN ISO 9001):**

*"Introduction*

*(...) The requirements for a quality management system specified in this document supplement the requirements for products and services. (...)*

*The following verb forms are used in this document:* ***"shall" indicates a requirement****; "should" indicates a recommendation; "may" indicates permissibility; "can" indicates a possibility or ability. (...)"*[12]

**Author's note**: The wording *"The requirements for a quality management system specified in this document supplement the requirements for products and services"* must not be taken to mean in DIN ISO 9001 that quality management representatives, auditors, and certification bodies would/may disregard legal requirements for products and services because these are regulated elsewhere.

This would contradict the requirements repeatedly stated in the text of the standard to comply with legal requirements and would make DIN ISO 9001 not only useless but even dangerous because it would undermine security. If this grammatically and teleologically justified interpretation of the text is not to be advocated by those responsible (Quality Management Representatives, auditors, certification bodies, etc.), this must be made clear to stakeholders.[13]

Furthermore, if a "*shall"* in the text of the standard implies a requirement, then a certification body must also guarantee that this requirement is met when issuing the certificate.

---

[9] Contrary to its misleading wording, ISO 9001 deals not only with products and "services," but also with work performance, trade, engineering, and much more, i.e., *any* type of service provision.
[10] See *Scherer*, Sustainable Management and Monitoring of Organizations (Governance) according to DIN ISO 37000, Successful Implementation, Auditing, and Reporting, Publisher DIN, DIN Media Verlag, 2025, Chapter 1.
[11] See *Scherer,* Successful Implementation, Integration, Auditing, and Certification of Compliance Management Systems According to DIN ISO 37301:2021, 1st edition, published by DIN, DIN Media-Verlag, 2022, , Introduction chapter.
[12] From DIN EN ISO 9001, Quality Management Systems – Requirements (ISO/DIS 9001:2025), Introduction section.
[13] See below 6.

*"1 Scope*

*This document specifies requirements for a quality management system when an organization a) needs to demonstrate its ability to consistently provide products and services* ***that meet*** *customer and* ***applicable statutory and regulatory requirements****, and*

*b) seeks to enhance customer satisfaction through the effective application of the system, including processes for improving the system and* ***ensuring[14]*** **compliance** *with customer requirements and* ***applicable statutory and regulatory requirements****. (...).*

*NOTE 2* ***Legal and regulatory requirements may also be referred to as legal requirements****. (...)".*

**Author's note**: The wording relating to "*legal and regulatory* requirements" is misleading and indicates a fundamental lack of understanding of compliance on the part of the standard's authors. Regardless of any standards, an organization must comply with "legal" or "mandatory" requirements simply because of its obligation to act lawfully. These *legal requirements* are more diverse than just legal or regulatory requirements.

They also include, but are not limited to, requirements from (EU) regulations, case law, technical developments (e.g., recognized rules or state of the art), and internally binding regulations (e.g., from guidelines/policies, works agreements, contracts, etc.).[15]

*"3. Definitions (...)*

*3.14 Requirement*

A requirement *or expectation that* is *specified, usually assumed,* or mandatory *(...) Note 4 on the term: Requirements can be established by various interested parties or by the organization itself.*

*3.15 Conformity*

*Fulfilment of a requirement (3.14) Note 1 to the term: The term "conformance" is a rejected synonym in English. The term "compliance" is a rejected synonym in French. (...)"*

**Author's note**: Due to the wording in Note 4 (*"Requirements may be established by various interested parties or by the organization itself.")* and the interpretation aid in Annex A ("*Annex A (informative) (...) A.3 Applicability (...) The applicable statutory and regulatory requirements mentioned in section 1a) are determined by the organization, taking into account those requirements that relate to the organization's ability to consistently provide compliant products and services through the effective application of the quality management system* (...)."**)** certification bodies, Quality

[14] In German contractual law governing breaches of performance, the term "assurance" is a so-called "indefinite legal term" with far-reaching (often negative) consequences for the assuring party, such as, under certain circumstances, no-fault liability for damages with no upper limit in the event that the assured characteristic is not present. Without knowledge of the meaning and scope of an increase in risk – which is not covered by insurance per se – a representation should not be made.

[15] See *Scherer,* Successfully Implementing, Integrating, Auditing, and Certifying a Compliance Management System in Accordance with DIN ISO 37301:2021, 1st edition, published by DIN, DIN Media-Verlag, 2022, chapter 4.5.

Management Representatives, lecturers, and auditors sometimes come to the incorrect view that the organization itself can arbitrarily establish the requirements to be audited and that the legally binding requirements no longer play a role.[16] After all, the interested parties also include the state with its legislative, executive, and judicial branches, which, among other things, monitor compliance with the principle of legality. In addition, the "or" in Note 4 is not to be seen as an alternative, but as cumulative.

The audit should therefore be conducted in exactly the opposite way:

Are the legally binding requirements identified and evaluated, and are activities to meet these requirements in place in the organization's processes and minds? And then: What other requirements, which do not contradict the above requirements, has the organization set for itself?

Incidentally, the fact that "conformity" is to be rejected in the English and French texts as a synonym for compliance or conformance is likely to stem from the standardizers' lack of understanding of compliance. No reason can be found for this incomprehensible view.

**Author's note**: Section 5 of the draft also contains clear mandatory requirements addressed to the bodies ("top management: e.g., board of directors/managing director") with regard to compliance requirements:

"*5.1.2 Customer focus*[17]

*Top management must demonstrate leadership and commitment to customer focus by:*

*a) customer requirements and* ***applicable legal and regulatory requirements are determined, understood, and consistently met***,

*b) the* risks *and opportunities that may affect the* ***conformity of products and services*** *and the ability to increase customer satisfaction* ***are determined and addressed***, *(...)."*

**Author's note**: Section 8 contains further mandatory requirements that correspond to the requirements of DIN ISO 37301, Section 4.5 Compliance obligations:

*"8.2.2 Determining requirements for products and services*

*When determining requirements for products and services to be offered to customers,* ***the organization must ensure that****:*

[16] Somewhat exaggerated, according to this – incorrect – view, the organization could stipulate that the product must meet a self-imposed security and compliance standard that does not correspond to the actual binding requirements. Upon identifying a corresponding process with this negative output, the auditor would then confirm: "Requirement fulfilled," and the certification body would issue a certificate ...

[17] From DIN EN ISO 9001, Quality Management Systems – Requirements (ISO/DIS 9001:2025), Section 5.1.2 "Customer Focus," p. 20.

*a) **the requirements for the product and service are determined, including: 1) any applicable legal and regulatory requirements**; (...)*

*8.2.3.1 The organization must ensure that it has the capability to meet the requirements for products and services offered to customers.*

*Before committing to supply a product to a customer or provide a service to a customer, **the organization must conduct a review that includes:***

*a) the requirements specified by the customer, (...)*

*b) **requirements not stated by the customer but necessary for the specified or intended use, as far as known**;*

*c) requirements specified by the organization;*

*d) **legal and regulatory requirements applicable to the products and services**;*

*e) requirements in the contract or order that differ from the requirements specified above.*

*8.2.3.2 Where applicable, **documented information shall be available as evidence of**:*

*a) the results of the review;*

*b**) any new or changed requirements for the products and services**. (...)"*

**Author's note**: Currently, there are many complex changes in European and German regulations relating to (IT and AI) (product) compliance:

Nothing remains unchanged, for example due to the AI Act, in particular the regulation of high-risk AI, changes to product liability law (AI or products with AI components are among the products within the meaning of the ProdHG and will also fall under the product definition of ISO 9001), for which a draft is already available, through the Product Safety Act and the EU Product Safety Regulation, through stricter circular economy and environmental criminal law, the Deforestation Regulation, the Green Claims Directive, the Cyber Resilience Act, and much more.

According to the AI Regulation, "prohibited AI" may no longer be used from 2025 onwards, subject to fines, and[18] from August 2026, high-risk AI will be regulated with the goal of protecting "human rights."

Note: Even simple AI—whether implemented as pure software or in other products—that is classified as not a risk under the AI Regulation may be considered "high-risk" in terms of product liability due to the danger to life and limb.

[18] The legal situation is uncertain due to a "digital omnibus" that is intended to amend the AI Regulation and the GDPR: See *Tagesspiegel Background*, "Digitization & AI, The Digital Omnibus – An Attempt at Classification," available at: https://background.tagesspiegel.de/digitalisierung-und-ki/briefing/der-digitale-omnibus-versuch-einer-einordnung

### 3.3 Liability responsibility for quality management systems without adequate compliance elements

Certification bodies, quality management officers, and internal auditors, as well as the managing director, confirm that the requirements of the quality management system are effectively met:

If regulatory requirements for products or services are not met and personal injury or property damage occurs, the liability of the executive bodies (board of directors, managing directors, supervisory board[19] ), managers, and quality management officers may be called into question, especially if it then transpires that the aforementioned responsible parties have only superficially addressed these requirements, if at all.

**Example**: In the *"Müller Brot*" case, according to media reports, *criminal investigations* were *also* conducted *against the heads of quality management* and production in the Munich area:[20]

*"(...) the Landshut public prosecutor's office is bringing charges against three former managing directors (...). Also in focus: the former plant manager,* ***the production manager, and the head of quality management.*** *(…)*"[21] .

**Example**: The "Transrapid" case[22] showed that in the absence of or having incorrect process descriptions, not only individual direct perpetrators, but also several responsible persons, in particular even simple supervisors, are the focus of investigations, charges, and convictions.

The liability of executive bodies and managers can become relevant in civil, criminal, and administrative fine law. The number of convictions of managers is rising steadily, and the latest case law regulates whether and when D&0 insurance can refuse coverage in the event of knowingly breaching duties, in particular cardinal duties.[23]

---

[19] Regarding the responsibility of a supervisory board member, see the recent Federal Court of Justice ruling of October 14, 2025 – II ZR 78/24, explained in Beck aktuell of November 27, 25, quote: *"(...) The court made it clear that monitoring does not only begin when risks become apparent. (...) According to Section 90 (1) sentence 1 no. 3, (2) no. 3 AktG, the management board must inform the supervisory board "regularly, at least quarterly" about the course of business and the situation of the company. (...) In the absence of reports, the supervisory board must not remain passive. It must actively request them and insist on structured information. (...) If formal reports are missing, as in this case, the supervisory board must follow up and, if necessary, exert pressure. This obligation applies to each individual member. (...) Unlike the lower courts, the court did not consider causality to be excluded. (...) According to Sections 116 and 93 of the German Stock Corporation Act (AktG), the burden of proof for lack of fault lies with the supervisory board (...).*"

[20] See *Ehrenstein*, When "greed and price pressure" prevail over hygiene, Welt, February 12, 2012, available at https://ww w .welt.de/dieweltbewegen/article13864527/Wenn-Gier-und-Preisdruck-ueber-die-Hygiene-siegen.html.

[21] Quote according to *Schweikl*, Müller-Brot scandal, BR, September 28, 2026.

[22] See *Werner*, Transrapid accident 2006: Suspended sentences for two train dispatchers, Mitteldeutsche Zeitung, March 3, 2011, available at https://www.mz.de/panorama/transrapid-unfall-2006-bewahrungsstrafen-fur-zwei-fahrdienstleiter-2268246.

[23] See *Scherer, Seehaus*, Duty of governance with early risk detection, resilience, and transformation as a cardinal duty of bodies and executives, ZInsO 31/2025, pp. 1515-1538, July 31, 2025, in German, available for free download at: https://www.risknet.de/elibrary/paper/pflicht-zu-governance-mit-risikofrueherkennung-resilienz-und-transformation-als-kardinalpflicht-von-organen-und-fuehrungskraeften/ and
*Scherer, Seehaus*, Manager liability, D&O insurance, and early risk detection in light of current case law, 2026, available for free download at Risknet.de.

### 3.4 Liability-exempting effect of a compliance management system

According to the highest court rulings, it is not a quality management system but a compliance management system (CMS) that has an exemption effect in these cases:[24]

Since 2017, various senates of the Federal Court of Justice, the European Court of Justice, and now also lower courts have ruled that a compliance management system can have a liability-exempting effect for organs and executives in the event of breaches of duty below management level.

### 3.5 Legally compliant quality management system

A look at sections 4.5 and 4.6 of ISO 37301[25] (CMS) is highly recommended for the legal certainty of the quality management system:

DIN ISO 37301:2021 (CMS) rightly requires in section 4.5 a *systematic* approach to identify and evaluate relevant, mandatory *compliance obligations* (current as well as new or changed requirements) and to ensure their (demonstrable) compliance with the compliance management system.

To this end, DIN ISO 37301:2021 defines in section 3.25 – *Compliance obligations*:

"*Requirements that an organization must comply with and requirements to which it voluntarily submits.*"

and regulates requirements regarding *compliance obligations* in section 4.5:

"*The organization must systematically identify its compliance obligations resulting from its activities, products, and services and assess their impact on its operations.*"

This is reminiscent of a *risk management process* for good reason*:* every violation or failure to comply with compliance obligations also represents a compliance risk, see ISO 37301 section 4.6.

### 3.6 Identification of compliance obligations and their risks

#### Identification of mandatory requirements

Identification must ensure that all requirements to be complied with, including international ones, are known, where relevant[26] .

---

[24] See *Scherer, Seehaus*, Duty of governance with early risk detection, resilience, and transformation as a cardinal duty of executive bodies and managers, ZInsO 31/2025, pp. 1515-1538, July 31, 2025, in German, available for free download at: https://www.risknet.de/elibrary/paper/pflicht-zu-governance-mit-risikofrueherkennung-resilienz-und-transformation-als-kardinalpflicht-von-organen-und-fuehrungskraeften/ *Scherer, Seehaus*, Manager liability, D&O insurance, and early risk detection in light of current case law, 2026, available for free download at Risknet.de.

[25] See *Scherer,* Successfully implementing, integrating, auditing, and certifying a compliance management system in accordance with DIN ISO 37301:2021, 1st edition, published by DIN, DIN Media-Verlag, 2022, chapters 4.6 and 4.7.

[26] See *Scherer, Butt, Reimertshofer*, Risks of international product liability from an entrepreneur's perspective in: Der Betrieb, issue 9 of March 5, 1998, pp. 469–474.

These requirements can be mapped in an agile and constantly evolving process-related *legal register.*[27]

It must be ensured that all future (new and changing) requirements are also identified and demonstrably complied with, even though this is a complex task:[28]

**For example***,* the *Federal Court of Justice* ruled that a dealer advertising with a photo of a *Ferrari* must state the CO2 emissions in accordance with the PKW-EnVKV (German Passenger Car Energy Consumption and Emissions Labeling Ordinance), even if they do not sell Ferraris at all.[29]

And here, too, *ignorance is no defense*, cf. the bookseller ruling.[30]

**Basic methodology for identifying mandatory requirements**[31]

First of all, many of the requirements that have already been identified and are continuously being re-identified on the basis of a corresponding process from a wide variety of technical and scientific disciplines (law, technology, ecology, etc.) must be "translated" into language that is understandable (not only for lawyers and technicians).

This leads to general difficulty, not only in technical product compliance, but also in healthcare, real estate, energy, etc., with regard to so-called *"indefinite legal terms"*[32] .

In the case of voluntary requirements ("should") relating to products and services, the *business judgment rule* (Section 93 (1) sentence 2 AktG) must be applied when making relevant decisions. Decisions should typically be based on the analysis and evaluation of data and information, and the reasoning behind decisions should be based on comprehensible, logical arguments and reliable data sources.[33]

An effective and efficient approach is to first define the company's divisions in terms of their functions/structural organization or (more modern) processes in terms of their operational organization.

The relevant requirements from legal areas and other mandatory requirements (from other sources)

---

[27] See *Scherer,* Successful Implementation, Integration, Auditing, and Certification of Compliance Management Systems in Accordance with DIN ISO 37301:2021, 1st edition, published by DIN, DIN Media-Verlag, 2022, chapters 4.6 and 4.7.

[28] See *Raum*, article "Compliance in connection with criminal and administrative fine obligations," in: *Hastenrath* (ed.), Compliance Communication, 2017, p. 33.

[29] See *Federal Court of Justice*, judgment of April 30, 2020 – I ZR 115/16.

[30] See *Federal Court of Justice*, judgment of October 18, 2020 – 2 StR 246/20

[31] See *Scherer*, *Ketelsen*, Technical Product Compliance, Bavarian Journal of Applied Sciences, 2022.

[32] See *BVerfG*, decision of August 8, 1978 – 2 BvL 8/77 and *Detterbeck*, Allgemeines Verwaltungsrecht mit Verwaltungsprozessrecht (General Administrative Law with Administrative Procedural Law), 18th edition, 2020, p. 105 et seq. and *Scherer*, *Ketelsen*, Technical Product Compliance, Bavarian Journal of Applied Sciences, 2022.

[33] In "0.2 Principles of Quality Management," "fact-based decision-making" is listed as one of seven principles, cf. DIN EN ISO 9001:2025-09, 0.2 QMP 6 "Fact-based Decision-making," but also A.6.2 "Quality Objectives and Planning to Achieve Them."

must then be assigned to these divisions or processes.[34]

The appendix to DIN ISO 37301:2021 (CMS) states the following in section A.4.5 – *Compliance obligations:*

"*The organization should identify compliance obligations by department, function, and different types of activities within the organization to determine who is affected by these compliance obligations.*"

Note: Mandatory requirements arise from a variety (!) of external (e.g., laws, case law, regulatory requirements, etc.) and internal (e.g., policies, contracts, instructions) sources.

**Risk-based approach**:

Since it is very difficult to always identify and fulfill all compliance obligations, you should start with the riskiest obligations based on a compliance risk analysis.

In this context, however, "risk-based" does not mean that less important obligations can be permanently ignored.

DIN ISO 37301:2021 states the following in Chapter A.4.5 – *Compliance obligations*:

*"A **risk-based approach** should be adopted, i.e., organizations should start by identifying the most important compliance obligations relevant to their business and then focus on all other compliance obligations (Pareto principle)."*

Note: The term Pareto principle, i.e., the "80/20 rule," is incorrect, even though it is stated as such in the standard. When it comes to compliance, less important issues must not be ignored.

### 3.7 Legal register

For the topic *of compliance in relation to performance (products, services, etc.)*, a type of (process-) topic-related (purchasing, sales, etc.) "legal register" should be created and maintained. This represents the relevant legal framework for this area.

DIN ISO 37301:2021 states the following in section A.4.5 – *Compliance obligations*:

*"Where appropriate, the organization should create and maintain a single document (such as a register or log) that lists all of the organization's compliance obligations and have a process for regularly updating the document."*

When assigning legal areas to the areas/processes, it becomes apparent that some legal areas/requirements (e.g., IT security requirements) occur in almost every area/process, while other requirements/legal issues are mainly focused on individual areas/processes (e.g., anti-corruption often in

[34] See *Scherer,* Successfully Implementing, Integrating, Auditing, and Certifying a Compliance Management System According to DIN ISO 37301:2021, 1st edition, published by DIN, DIN Media-Verlag, 2022, chapter Introduction – *"Doing the right thing right"* and chapter 8.1 – *Digitization and enrichment of the various management, core, and support processes*.

purchasing and sales).

However, a document, Excel file, etc. containing countless legal requirements is not sufficient to ensure compliance with legal requirements:

These regulations must still be translated into understandable language and process steps for fulfilling the requirements and implemented in the structural and procedural organization and in the minds of the respective (compliance) risk owners:

**Implementation of activities to fulfill the requirements in the processes**

Once it has been determined or decided which *specific* requirement (prioritized) is to be fulfilled, process steps, activity and competence transfer measures must be derived, implemented in the processes, and made effective to ensure that the requirement is/was fulfilled in a measurable, audit-proof, and documented manner.

This can be achieved with leading workflows, automation, digital process twins[35] , and corporate culture, awareness, competence (knowledge, understanding, ability, and willingness), as well as an effective "lines of defense" control and monitoring system.

When assigning mandatory requirements to processes, the *RACI method* should be considered: The respective process users, those "responsible" (R), should be aware of and observe the requirements in their process. The "process owners," i.e., those responsible for timeliness, compliance, etc. (those accountable (A)), e.g., sales management for sales processes), should ensure, with the support of the specialists (consulted (C)), that the respective process always meets all relevant requirements. The relevant stakeholders (informed) should always be informed about process changes.

### 3.8 Risk assessment with regard to mandatory requirements

Depending on the extent of non-compliance with mandatory requirements—e.g., in the event of danger to the life and limb of third parties or environmental hazards—this can lead to the destruction of the organization and the responsible bodies and/or employees, imprisonment, fines, and claims for damages, including loss of reputation.[36]

Risk assessment must also be carried out *appropriately* for compliance risks (!), i.e., in accordance with recognized scientific and practical standards: Quantification, aggregation, and consideration of

[35] See *Rieger, Scherer*, The Digital Process Twin in Healthcare – also as a contribution to sustainability (ESG, CSR), systemic livelihood security (resilience) and governance in: Journal für Medizin- und Gesundheitsrecht, issue 2-2021 (available for free download at scherer-grc.net/publikationen).

[36] See *BAG*, ruling of April 29, 2021, Ref.: 8 AZR 246/20 and United States District Court for the District of Columbia, Consent Decree Civil Action Nos. 1:20-cv-2564, 1:20-cv-2565, September 14, 2020, p. 41 et seq., available online at: https://www.epa.gov/enforcement/daimler-ag-and-mercedes-benz-usa-llc-clean-air-act-civil-settlement-consent-decree (last checked: September 25, 2021).

risk-bearing capacity are now required by law, state of the art, and many standards.[37]

### 3.9 Risk management with regard to mandatory requirements

For risk management, it is necessary to continuously raise awareness of the company's orientation and compliance culture among employees through regular training and an established "tone from the top" so that they always act in accordance with the CMS.[38]

The implementation and effectiveness of activities to ensure compliance with obligations in the processes is much more effective than simply issuing guidelines and the like.

The "lines of defense" model with compliance, risk management, ICS, and audit[39] , the establishment of (AI-supported) monitoring processes[40] , and neutral ombudspersons[41] should ensure monitoring and maturity assessment. This also identifies risks of deviations from specifications and derives activities for improving the process and its components.

## 4. "Risk- and opportunity-based thinking": Appropriate presentation of the mandatory requirements for risk management in quality management: None

The draft of the new DIN ISO 9001 refers to *"risk-based thinking"* in the introduction, Annex A, various other places in the standard:

*"Introduction*

*0.4 Relationship to other management system standards*

*This document applies the harmonized structure to achieve alignment of ISO management system standards. This document enables an organization to apply the process-oriented approach in conjunction with the PDCA cycle,* ***risk-based thinking****,* ***and opportunity-based thinking*** *to align or integrate its quality management system with the requirements of other management system standards. (...)."*[42]

*"Annex A (informative) (...)*

*A.6.1.2* ***Risk-based thinking***

---

[37] See *Scherer, Seehaus*, Duty of governance with early risk detection, resilience, and transformation as a cardinal duty of organs and executives, ZInsO 31/2025, pp. 1515-1538, July 31, 2025, in German, available for free download at: https://www.risknet.de/elibrary/paper/pflicht-zu-governance-mit-risikofrueherkennung-resilienz-und-transformation-als-kardinalpflicht-von-organen-und-fuehrungskraeften/ *Scherer, Seehaus*, Manager liability, D&O insurance, and early risk detection in light of current case law, 2026, available for free download at Risknet.de and *Scherer*, *Romeike*, *Gursky*, More risk competence for a new world in: *Journal für Medizin- und Gesundheitsrecht* (Journal of Medical and Health Law), issue 3-2021, pp. 159–165.

[38] See *Scherer*, *Fruth* (eds.), Governance Management Volume II (Standard & Audit), 1st edition, 2015, p. 130.

[39] See ibid., pp. 188–189.

[40] See *Noack*, Artificial Intelligence and Corporate Management in: Festschrift for Christine Windbichler on her 70th birthday on December 8, 2020, p. 956.

[41] See *Scherer*, *Fruth* (eds.), Governance Management, Volume I, 2015, p. 186.

[42] See DIN EN ISO 9001 Quality Management Systems – Requirements (ISO / DIS 9001:2025-9), Introduction section.

*(...) This document specifies requirements for the organization to understand its context (see 4.1) and determine the risks as a basis for planning (see 6.1). This embodies the application of risk-based thinking in the planning and implementation of quality management system processes (see 4.4) (...).*
*Although 6.1 specifies that the organization must plan actions to address risks,* ***no formal risk management methods or documented risk management process are required. Organizations may decide to develop a more extensive risk management approach than required by this document,*** *e.g., by applying other guidelines or standards.*
*NOTE 1 See ISO 31000 [9] for guidance on risk management.*
*NOTE 2 See ISO 31073 [10] for terms used in risk management. (...)"*[43]

Even in the new version of DIN ISO 9001, "*risk-based thinking*" remains incomprehensible, legally questionable, and impractical.

The general *"risk-based approach"* which is also recognized by case law and auditors—means that, based on an appropriate risk analysis, the important things must be dealt with first/prioritized.

The management of risks to life and limb, personal sanctions against employees, and financial losses that would impair the risk-bearing capacity of the organization are the top priorities. The mere requirement for *"risk-based thinking" without also* including *risk-based decision-making and corresponding action* is foreign to the recognized rules of technology in risk management.

When "*measures for dealing with risks and opportunities*" are required, this must also include compliance risks.

There is no objective reason to exclude such a large field with risks that could potentially threaten the existence of the company. This would also be contrary to duty within the meaning of Sections 43 GmbHG, 93, 116 AktG, cf. LG Munich ("Neubürger ruling").

It is downright paradoxical and legally misleading to demand risk-based thinking and the planning of measures to deal with risks on the one hand, and on the other to make the inaccurate and "dangerous" statement:

*"Although 6.1 stipulates that the organization must plan measures to deal with risks,* ***no formal methods for risk management or a documented risk management process are required. Organizations can decide whether they want to develop a more extensive approach to risk management than is required by this document,*** (...)".

[43] See DIN EN ISO 9001 Quality Management Systems – Requirements (ISO / DIS 9001:2025-9), Appendix.

This statement is probably due to fear of competition from risk management standards or from subject matter that is completely new to quality management, especially when compliance risks are considered.[44]

However, if customer satisfaction is the goal of ISO 9001, then the customer's business partner should have an appropriate risk (and business continuity) management system in place to ensure that it does not experience an operational disruption or crisis that would jeopardize the fulfillment of its contractual obligations: Ensuring security of supply is one of the main objectives of modern supplier screening and an indispensable prerequisite for customer satisfaction.

[45]Contrary to the wording of the new standard, measures for dealing with risks must always be planned appropriately and in accordance with legal requirements. A clarifying note should have been included here to indicate that there are numerous mandatory requirements for early risk detection and management in laws, case law, recognized rules of technology, etc., which are binding.

**Example** of an inappropriate risk assessment method borrowed from quality management and based on the old version of FMEA[46] , proposed in a standard work[47] for quality management:

The following scenario is assumed:

The risk of a possible product defect, which is likely to occur only once a year (category Exposure (E) rare: (E) value 1 (from 0.5 to 10)) with a low probability (W) ("not very common": (W) value 3) and the second-highest severity (S): "extremely serious" "e.g., one fatality" (S) value 15 (from 1 to 40) has been identified and assessed. According to the (incorrect) assessment that one fatality should not immediately lead to the highest damage assessment, and as a mathematical product with three factors, the (incorrectly) assessed risk priority number (RPN) in the example would be 45 (1 x 3 x 15) with the recommended action of only: "*Caution* advised," but not the next levels: "*Action* required" (70 to 200) or even "*Immediate improvement* essential" (200 to 400) or the highest level (400 and above): "Act immediately!"

– If the risk documented in this way were to materialize, the public prosecutor's office and the court would assume not negligent but intentional homicide: A fatality was considered possible and – due to incorrect assessment – was accepted. This is conditional intent: Dolus Eventualis.

[44] See DIN EN ISO 9001, Quality Management Systems – Requirements (ISO/DIS 9001:2025), Section 6.1 "Measures for dealing with risks and opportunities," p. 21.
[45] See Section 1 StaRUG.
[46] Failure mode and effects analysis.
[47] See the 3rd edition of an otherwise excellent work published by DIN and Beuth Verlag on: Successful Quality Management according to DIN EN ISO 9001:2015, in which a method borrowed from FMEA was used from QM for risk assessment. This example is no longer included in the newer editions. The VDMA has also corrected its FMEA method in the meantime.

## 5. "Process-oriented approach": Appropriate presentation of the requirements for process management in quality management: None

In the draft of the new DIN ISO 9001, the "process-oriented approach" occupies a special place in the text of the standard:

*"Introduction*

*0.3 Process-oriented approach*

*0.3.1 General*

*This document promotes the implementation of a process-oriented approach to establishing, implementing, and improving the effectiveness of a quality management system in order to increase customer satisfaction by meeting customer requirements. Specific requirements that are essential for the implementation of a process-oriented approach are contained in 4.4. (...)*

*The process-oriented approach involves the systematic determination and control of processes and their interactions so that the intended results are consistent with the quality policy and strategic direction of the organization.* ***Control of the processes*** *and the system as a whole* ***can be achieved through the PDCA cycle (see 0.3.2), which focuses on risk-based thinking (see A.6.1.2) and opportunity-based thinking (see A.6.1.3) to take advantage of opportunities and prevent undesirable outcomes.*** *(...)"*[48]

*"5 Leadership*

*5.1 Leadership and commitment 5.1.1 General*

*Top management shall demonstrate leadership and commitment to the quality management system by:*

*a) ensuring that the quality policy and quality objectives are established and consistent with the strategic direction of the organization;*

*b)* **ensures that the requirements of the quality management system are integrated into the organization's business processes***; (...).*[49]

Although process management is still often treated as an afterthought to quality management by quality management officers, its importance has increased significantly due to digitalization and AI support. Because of this, it would be worthwhile for management to attach greater importance to process management.

The requirements for processes and process management are primarily defined by law.[50] Merely relying on "risk-based thinking" without process compliance management that ensures legal certainty does not "prevent" "undesirable results" in the sense of compliance violations.

[48] See DIN EN ISO 9001, Quality Management Systems – Requirements (ISO/DIS 9001:2025), Introduction section.
[49] See DIN EN ISO 9001, Quality management systems – Requirements (ISO/DIS 9001:2025), section 5.1.1.
[50] See, for example, the "Transrapid decision" and requirements for a legally compliant organization in *Scherer*, Sustainable Management and Monitoring of Organizations (Governance) according to DIN ISO 37000, Successful Implementation, Auditing, and Reporting, published by DIN, DIN Media Verlag, 2025, Chapter 4.2, p. 74.

The Transrapid case mentioned above[51] showed that, in the event of corresponding failures in process management, not only individual direct perpetrators but also several responsible parties, particularly line managers, are the focus of investigations, charges, and convictions.

Each of the approximately 20 (process) subject areas of an organization represent a main process area as part of the company-wide process landscape (e.g., the sales process, which should be networked with the other process areas). [52]

Each main process area can be represented as a flowchart (in outdated form still found in Excel, Word, or PowerPoint, modeled according to the state of the art in BPMN 2.0) with an associated description of input and output, process steps, process execution managers, owners, or managers (cf. RACI), applicable documents, compliance requirements and risks, control points, etc. It consists of further sub-process areas (e.g., for the main process "Sales": marketing/acquisition, inquiry management, customer creation, etc., through to after-sales, product monitoring, and complaint management).

The process-oriented approach is required by current standards, not only the new ISO 9001, but also, for example, DIN ISO 37000 (governance).[53]

Processes are descriptions of procedures. The appropriate level of detail in a process description depends, for example, on how often a process is executed and who or how many people are involved in it.

An essential prerequisite for recognizing the digitization potential of processes is to first consider the current status quo. Since processes are often not documented or not documented up to date, they must first be modeled.

Integrated human workflow management systems are necessary for a "true digital transformation"[54]

.

[51] See *Werner*, Transrapid accident 2006: Suspended sentences for two train dispatchers, Mitteldeutsche Zeitung, March 3, 2011, available at https://www.mz.de/panorama/transrapid-unfall-2006-bewahrungsstrafen-fur-zwei-fahrdienstleiter-2268246.
[52] See *Scherer*, Sustainable Management and Monitoring of Organizations (Governance) according to DIN ISO 37000, Successful Implementation, Auditing, and Reporting, published by DIN, DIN Media Verlag, 2025, Chapter 8.1.
[53] See *Scherer*, Sustainable Management and Monitoring of Organizations (Governance) according to DIN ISO 37000, Successful Implementation, Auditing, and Reporting, Publisher DIN, DIN Media Verlag, 2025, chapter " Introduction " and chapter "8.1 „ ."
[54] See *Scherer*, Compliance Management System according to DIN ISO 37301:2021 – Successful Implementation, Integration, Auditing, Certification, DIN Media, 2022, Chapter 8.1: Excursus: Implementation of Governance Measures and Projects and Processes Enriched with Governance Components .

The following figure symbolically shows how a standardized core process (according to ISO 9001:2015) could be modeled based on BPMN 2.0. The section at the bottom, the "IT systems" swim lane, is intended to show that various IT systems are used when performing the individual process steps. The figure also shows that, in addition to a wide range of specialized IT systems (SAP/Office/documentation system/CRM, etc.), a wide variety of digitalization and AI components, as well as people, can be used at different points in the process landscape.

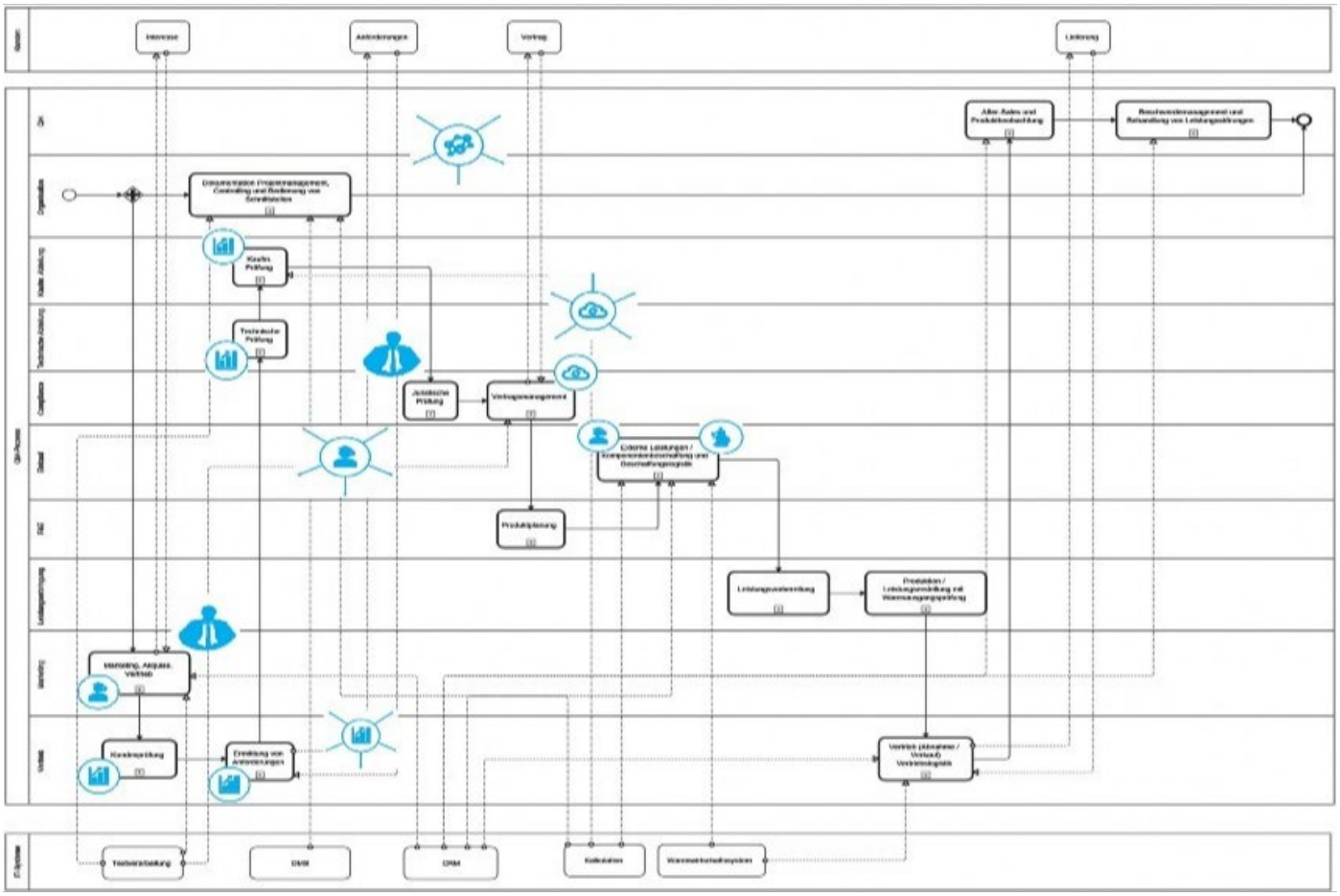

*Figure 1: People and components of digitalization in the process landscape*[55]

Artificial intelligence is also likely to fundamentally change business process modeling (BPM). This will also result in an adjustment of the BPM modeler tool market. These developments must be kept under constant review.

Most business activities take place as processes. In the future, some of these will still be carried out by humans. In order to do the right thing at the process level, it is also extremely important for management and employees to have the right attitude on a cognitive and emotional level: *tone from*

[55] Own representation from *Scherer*, Compliance Management System according to DIN ISO 37301:2021 – Successful Implementation, Integration, Auditing, Certification, DIN Media, 2022, Chapter Introduction.

*the top*, culture, awareness, skills, motivation, and much more. Only then can a process organization become effective ("lived").

DIN ISO 9001 emphasizes that a QM system consists of interacting processes that together form a process system. This standard explicitly promotes the use of a process-oriented approach, including the development, implementation, and improvement of the effectiveness of a quality management system to increase customer satisfaction by meeting requirements.[56] The new standard explicitly requires consideration of (compliance) risks and opportunities in relation to processes and results. Measures for dealing with risks and opportunities must be integrated into the processes of the quality management system and implemented effectively there.

[56] Based on DIN EN ISO 9001 (current version), foreword and section 0.1/0.2 on process-oriented quality management systems.

## Check: The maturity level of process management: Where is your organization currently and where should it be (in the near future)?

**Evolution stage 1: The process does not yet exist or only exists in people's minds**

There may be "good processes" in the minds of "old hands," but they are not documented.

Danger: What happens when these employees are gone (due to illness or retirement)?

**Evolution stage 2: From the mind to the document (analog or digital)**

If knowledge and expertise are documented (up to date), ideally it could also be used by others (colleagues/successors/trainees). In practice, this includes versions in paper and analog file folders, as well as PDF documents, Excel files, and much more...

**Evolution stage 3: Visualize process steps and assign all relevant information to the individual process steps**

Visualized process steps with relevant information available "on site" help people to "know" and "understand." In practice, components that ensure compliance with QM, risk, compliance, ICS, or audit requirements are very often still missing from the respective process steps.

**Evolution stage 4: Enriching processes with risk, ICS, or compliance elements.**

The processes must be enriched with activities to fulfill the requirements of QM, risk, compliance, ICS, or auditing. Experience shows that processes modeled by the relevant process step owners (R and A) are more likely to be accepted and implemented. However, digital process manuals in Excel, Word, and other "dead" documents are no longer state of the art. Instead, state of the art in process management and, for example, in IT security law, data protection, or occupational safety are (partially) automated, leading processes:

**Evolution stage 5: Modeling processes with Business Process Management (BPM 2.0) and linking them to a repository (data room)**

Process modeling in BPMN 2.0 is state of the art. The many competing modeling tools on the market[57] enable accountable parties to update their processes themselves at any time without the need for expensive IT specialists.

[57] ADONIS, iGrafx, Intellior, ARIS, Signavio, Visio, GBTEC, Camunda, Bizagi, Confluence, ProcessMaker, Omni-Tracker, etc.

Now, the right applicable documents (sample forms, checklists, etc.) must also be available for each process step. This is ensured by digitally networking all activities to fulfill the requirements contained in the elements of laws, norms, standards, and guidelines with a so-called "repository."

**Evolution stage 6: Bringing the modeled process to life through partial automation and enrichment with *artificial intelligence*[58]**

However, the modeled/drawn process is not yet alive: In the next stage, processes are fully or partially automated, or workflows guide employees through their tasks. AI agents support and execute routines independently.

**Evolution stage 7: "Integrated combined management system on demand" with compliance, QM, risk, ICS, information security management system, etc.:**

For management and employees, many parallel "island systems" mean an unworkable (ineffective) and expensive bureaucracy.

Converting an existing management system to an interdisciplinary, integrated GRC management system is simple and achieves high value contributions.

Not only individual processes or parts of isolated management systems, but the entire integrated GRC management system runs automatically or is managed via human workflows.

The "dogmatic approach" to enabling a digitized integrated management system consists of focusing on the *end-to-end process*: Activities to fulfill the relevant requirements of various laws, standards, etc. from various cross-cutting topics such as compliance, quality management, risk, sustainability, etc. are integrated into the various sub-processes, see point 6 below. Compliance, quality management, risk, sustainability, etc. are integrated into the various sub-processes, see point 6 below.

[58] See *Rieger, Scherer,* The Digital Process Twin in Healthcare, JMG 2/2021, pp. 83–91, available for free download at Scherer-grc.net/Publikationen

## 6. Presentation of the requirements for an integrated ESGRC management system: Not applicable

The new version of DIN ISO 9001 is more closely aligned with the Harmonized Structure in order to enable the integration of "management system islands," but does not explain how this should be implemented in concrete terms.

This still allows some consultants, auditors, certifiers, etc. to "sell" their numerous, costly, and uncontrollable island management systems.

*"Introduction (...)*

*0.4 Relationship with other management system standards*

***This document applies the harmonized structure** to achieve alignment of ISO management system standards. **This document enables an organization** to apply the process-oriented approach in conjunction with the PDCA cycle, risk-based thinking, and opportunity-based thinking to **align or integrate its quality management system with the requirements of other management system standards**. (...) This document does not contain specific requirements for other management systems, e.g., for environmental management, occupational health and safety management, or financial management. (...)"*

An organization that gradually introduces one or the other "management systems" almost inevitably produces isolated solutions that are not put into practice. Due to a lack of homogeneity, the data from these systems (if it is entered at all) is not adequately available for the possibilities offered by modern digital data analysis, among other things.

Current environmental developments and mandatory legal requirements call for an integrated approach that resolves the complexity and cost burden for organizations.

Converting a quality management system to an integrated ESGRC management system is simple and delivers high value.

It will become apparent that the many different standards for management systems can be broken down into redundant or analogous elements.

It is estimated that there is around 70% overlap here: for example, the interested party’s analysis is only carried out once. Due to the redundancies in other standards, it can be used for quality management, risk management, compliance management, business continuity management, etc.

Since almost all standards (ISO, COSO, IDW, DIIR, etc.) for management systems can be condensed into a uniform, largely redundant structure and content, companies should take the opportunity to convert their existing (quality) management system into a holistically integrated management system that not only covers individual topics but also enables compliance with the

requirements of proper organizational management and monitoring, i.e., governance, as a whole. The effort involved is manageable:

**Example**: **The enrichment of a process flow with activities to meet the requirements of various regulations and standards as an example of an "integrated management system"**: The *quotation management process* as part of the sales process is examined here **as an example**. The integration of risk or compliance components into existing process flows can be illustrated very nicely using the example of customer verification (KYC: Know Your Customer), namely identity, creditworthiness, and legality checks (e.g., foreign trade controls and money laundering at the customer) as one of the first steps in the quotation process. This step not only reduces risks and avoids personal liability but also shows that governance with risk and compliance management helps to save a lot of money.

Identity verification clarifies the question of who the actual contractual partner is (Hans Maier (spelled with ai, ei, ay, ey ...?) or Hans Maier Bau-GmbH or Hans Maier Holding GmbH & Co. KG or Hans Maier Bauleistungen AG). Often, communication is only conducted with "Fa. Maier" or even using different letterheads. Claims against the contractual partner would be virtually unenforceable due to the unresolved question of who the actual partner is.

In the current climate of embargoes, etc., the "beneficial owner" must also be checked.

The power of representation of the person acting on behalf of the contractual partner can also be clarified at this point. It must be checked whether the person acting on behalf of the contractual partner is sufficiently authorized, for example, by power of attorney, power of representation, or individual power of attorney.

The credit check shows whether the probability of receiving payment is high enough to even want to make an offer; for example, if the figures of the inquiring limited liability company are good, but this limited liability company is part of a group in crisis (risk of infection).

The legality check (foreign trade law, export control, money laundering law, etc.) provides information on whether an offer may be submitted at all.

Sustainability characteristics and respect for human rights also often play a role in contract partner checks.

The same applies, for example, to IT governance issues, such as where our data ends up and whether IT services can be easily shut down (digital sovereignty).

In practice, the corresponding review steps are often completely missing, are often only carried out for new customers, or are located at an unfavorable point in the process flow, for example, only after technical and commercial reviews and contract negotiations have been carried out, which wastes a lot of time and money.

With regard to creditworthiness, identity, and legality checks on customers, moving the process step to the first place in the quotation process has the effect of reducing financial risk and liability.

For example, it is important to prevent the organization's portfolio from being jeopardized by a significant bad debt loss from a customer with poor creditworthiness. In addition, in the event of a significant financial loss due to a lack of creditworthiness checks, the managing director of the company would be personally liable for breach of organizational duty: Failure to carry out a creditworthiness check has already been considered a breach of duty by management in case law, and as a result, a claim for damages against the managing director was constructed under Section 43 (2) GmbHG (German Limited Liability Companies Act).[59]

Adding the step of "customer verification" (identity, creditworthiness, and legality checks, such as foreign trade law and money laundering law) to the process at the optimal point, namely immediately after the customer who has requested a quote has received confirmation of receipt of their letter, has positive effects.

If the information is negative, no time-consuming and costly technical and commercial checks or contract preparation are carried out, thus saving several thousand euros/dollars. Instead, due to the free capacity, the offer for a "positive" customer, who might have switched to a competitor due to the slow processing times that were normal in the past, is processed promptly and successfully implemented.

**Note**: The KYC sub-process also fulfills requirements from quality, risk, compliance, and sustainability management, from the internal control system, and much more. It also fulfills the relevant regulatory requirements, recognized rules of technology, and standards.

This kills many birds with one stone; it is an integrated management system in action.

And it continues accordingly, namely with the analysis and optimization of all other important processes by enriching them with steps to meet the requirements of risk and compliance management, etc.

[59] For the personal liability of the managing director for failing to carry out a credit check, see, for example, the case law on Section 43 (2) GmbHG (Neubürger decision of the Munich Regional Court, further references in the bibliography).

## 7. Reference to potential increase in liability risk due to the management of quality management system certificates[60] : None

The trend toward certification continues unabated and is intended to enable verification of compliance with standards and lead to competitive advantages over non-certified organizations.

**Number of ISO 9001 certificates in Germany and worldwide according to ISO Survey 9/2025**:

Quote: "(...) *At the end of 2024, there were 1,474,118 ISO 9001 certificates at 2,321,640 locations worldwide. Last year, 837,052 certificates were reported, so the quality of the data appears to have improved significantly.*

*According to this evaluation, Germany has risen from 41,760 to 45,983 certificates at 104,193 locations, which represents an increase of 10% or even 64%. However, as mentioned above, this figure is not verifiable or representative.*

*ISO 9001 ranking worldwide*

*China ranks first with 651,851 certificates, as in previous years. This data is considered reliable as it comes from the official government agency this year. Italy ranks second with 101,426 certificates. India ranks third with 95,007 certificates, followed by Korea with 51,647 certificates. Germany ranks fifth, followed by Spain, Japan, Great Britain including Northern Ireland, and America in ninth place ahead of Brazil*.[61]

A functioning QM system can also be of considerable importance in defending against contractual disputes or administrative or legal proceedings.

Example (Verden Regional Court):

A client of the author was sued for an alleged production error. According to the case law of the Federal Court of Justice, proof of a so-called "outlier" is necessary to exonerate oneself, as there is no liability for accidental production errors. Thanks to the documented and certified testing measures as part of the effective quality management system, the company was able to prove that production was of high quality and that there were no abnormalities in the series. The possible defect was therefore a harmless outlier. Result: Dismissal of the lawsuit – economic advantage in the six-figure range.

At the same time, a new risk arises:

---

[60] See *Scherer, Friedrich*, "Increased Risk through Certification of Quality and Risk Management Systems," in: ZfAW 10th year (2007), pp. 15–19, available for free download at: https://www.schererrecht.de/images/Veroeffentlichungen/Risikoerhoehung_durch_Zertifizierung/Beitrag_ZfAW.pdf.

[61] See *Gertz*, ISO Survey 2024 – DakkS refuses data transfer, Qualitätsmanager aktuell dated November 21, 2025, available for free download at: https://www.qm-aktuell.com/zeitschriften/iso-survey-2024-dakks-verweigert-datentransfer/ Quote: *"The ISO Survey was published at the end of September, summarizing the ISO certificate figures and the number of locations with certificates as of December 31, 2024. (...) The certification bodies accredited by the German Accreditation Body (DAkkS) were unable or unwilling to provide their data for the ISO survey to IAF CertSearch. Even though some other German certification bodies submitted their data directly to CertSearch, the results do not therefore reflect the entire German market."*

Initial, surveillance, or recertification audits are often not risk-based, i.e., based on an appropriate analysis of where the real problems lie. Many organizations only bring themselves into a "certifiable state" in the short term and, after receiving the certificate, neglect the necessary maintenance of the QM system.

In addition, holding a certificate can result in higher legal requirements. Failure to meet these requirements can have significant consequences for companies and, in some cases, their management.

A certificate merely confirms the introduction of a system in accordance with a standard – it is no guarantee of "100% quality" or "zero risk."

As long as certification remains purely internal, it does not automatically increase liability.

However, problems arise when companies advertise with the certificate (website, packaging, letterhead, etc.) or when the provision of a certified management system becomes part of a contract.

According to Section 276 (1) of the German Civil Code (BGB), the standard of care increases when certification is highlighted in advertising. A company that publicly advertises its certificate must demonstrate a higher standard of care than a non-certified company.

If certificates are publicly advertised, the corresponding processes must actually have been carried out, as otherwise there is a risk of liability under the warranty for material defects (§ 434 ff. BGB).

This may even be the case without any specific quality defects being demonstrable if the non-application of the advertised QM system already constitutes a material defect.

Public statements that create the impression of a guaranteed characteristic can be interpreted as a warranty—with significant consequences in terms of strict liability and reversal of the burden of proof in favor of the warranty beneficiary.

Therefore, formulations such as "*Our certified QM system ensures the faultlessness of our products*" or similar should be avoided.

If the use of a certified QM system has been agreed in quality assurance agreements or other contracts, damage and weaknesses in the system may result in damages for breach of duty (Sections 280, 281 BGB), an extraordinary right of termination (Section 314 BGB), possible contractual penalties, and lump-sum damages.[62]

[62] See *Scherer, Friedrich*, "Increased risk through certification of quality and risk management systems," ZfAW 10th year (2007), pp. 15–19, available for free download at: https://www.schererrecht.de/images/Veroeffentlichungen/Risikoerhoehung_durch_Zertifizierung/Beitrag_ZfAW.pdf.

A management system that is not implemented can result in significant sanctions, including personal liability for the management and other responsible executives.

## 8. Presentation of the new requirements for management systems, managers, employees, auditors, management system and personal certifications: None

One means of demonstrating the appropriate professional competence of QM officers and QM auditors is through appropriate personal certifications.

*Personal certifications for QM auditors* serve as formal proof that a person has the necessary technical, methodological, and personal competence to professionally audit quality management systems such as DIN EN ISO 9001.

The basis for the content of such certifications is primarily ***ISO 19011***[63] , which *contains* audit principles, the audit process, and*, **in section 7**, **recommendations on the competence requirements for auditors**, including knowledge of ISO 9001, industry knowledge, confident mastery of audit methods, and personal qualities such as integrity and communication skills.*

*ISO 19011 is currently undergoing a fundamental revision*:

*"(...) Expected changes to the new ISO 19011:*

*Remote audits and digital technologies, Extension by adding remote audit methods in relation to ISO/EC TS 17012:2024 (guidance for remote audits), Guidance on planning and conducting remote audits and information on technologies, Guidance for virtual sites, Harmonization with other ISO standards, Standardization of terms and definitions, **Orientation towards the Harmonized Structure (HS)** of ISO management systems, **Strengthening of the risk-based approach, Targeted prioritization of high-risk areas in audit planning and implementation**, Greater attention to topics such as climate risk and digital systems, Editorial revision of the standard*

*What is the next step in the revision process?*

*A draft of the ISO DIS 19011:2025:3 guideline is currently being discussed among international experts. The German text of this draft is also available as DIN EN ISO 19011:2025-04 from April 2025. **The final version of the guideline is expected to be available in early 2026**. (...)"*[64]

***ISO/IEC 17024 describes the requirements for certification bodies that certify individuals**,* regulates the development of certification schemes, testing procedures, independence, validity of

[63] See DIN EN ISO 19011 Guidelines for auditing management systems (ISO 19011:2018), Section 7 "Competence and evaluation of auditors."
[64] See *Gut Cert*, Revision of the ISO 19011 audit guideline, 24.9.2025, available for download on the Internet.

assessment, and regular recertification, and thus serves as a normative basis for external auditor certificates.[65]

For auditors who audit management systems on behalf of accredited certification bodies (DakkS), the requirements of the ISO/ IEC 17021 series, in particular ISO/IEC 17021-1 on the structure and impartiality of certification bodies and **ISO/IEC 17021-3 on the specific competence requirements for auditors of quality management systems**, which specify how qualifications, experience, and audit practice must be systematically assessed and monitored.[66] While ISO 19011 itself does not specify a formal certification or accreditation system, the combination of these standards creates a consistent framework that ensures that QM auditors perform their tasks in a technically sound, independent, and traceable manner, with formal personal certifications playing an important role, particularly in the context of external audits. In light of the upcoming ISO 9001:2026, these examinations and certifications intended for QM officers and QM auditors should now also cover the above-mentioned topics ***of process, governance, risk, and compliance management competencies*** in order to be appropriate and risk-based.

## 9. Conclusion

**The new DIN ISO 9001 offers many opportunities when applied critically and correctly but also poses considerable risks when applied without reflection and without GRC competencies.**

**The current transformation in all areas also requires a fundamental rethinking of quality management.**

**Prof. Dr. jur. Josef Scherer**

[65] See DIN EN ISO/IEC 17024 Conformity assessment – General requirements for bodies operating certification of persons (ISO/IEC 17024:2012).
[66] See DIN EN ISO/IEC 17021-3 Conformity assessment – Requirements for auditing and certification of quality management systems (ISO/IEC 17021-3:2017).

Prof. Dr. jur. Josef Scherer is a lawyer and consultant, founder (2012) and director of the International Institute for Governance, Management, Risk and Compliance Management, and head of the ESGRC administrative department at the Deggendorf Institute of Technology (THD). Since 1996, he has been a professor of corporate law (compliance), risk and crisis management, restructuring and insolvency law at the THD. Previously, he worked as a public prosecutor at various regional courts and as a judge at the regional court in a civil chamber.

In addition to his work as senior partner at the law firm Prof. Dr. Scherer & Partner mbB, which specializes in commercial law and governance, risk, and compliance management (GRC), he prepares scientific legal opinions and acts as a judge in arbitration proceedings.

From 2001 to 2024, he also worked as an insolvency administrator in various local court districts.

Prof. Dr. Scherer serves as a compliance ombudsperson or external compliance officer for various companies and corporations. He is a sought-after speaker at management training courses in renowned companies as well as in the continuing education program of the BR-alpha television station and the Virtual University of Bavaria (VHB).

In cooperation with TÜV, he designed the renowned and accredited part-time master's program in Risk Management and Compliance Management at THD, which has been running for over 15 years, and heads the certificate course "Sustainability and GRC" as well as the part-time bachelor's program "Sustainability, Governance, and Digitalization."

Since 2015, Prof. Dr. Scherer has been a member of the advisory board of the Institute for Risk Management and Regulation (FIRM), Frankfurt (www.firm.fm).

Since 2016, he has been a member of the DIN Standards Committee for Services (Working Committee NA 159-01-19 AA) for the development of ISO/DIN standards in human resource management, and since 2017, he has been a member of the ISO TC 309 Governance of Organizations delegation (Working Committee NA 175-00-01-AA) for the development of ISO/DIN standards in the field of corporate governance, compliance, and whistleblowing.

Since 2016, Prof. Dr. Scherer has been Technical Director of the "User Group Sustainable Corporate Governance (ESG/CSR/GRC) and Compliance" at Energieforen Leipzig, and since 2018 a member of Working Group 252.07 of Austrian Standards International for the development of ÖNORM D 4900 ff. (risk management system standards) and has been a member of DICO (German Institute for Compliance e. V.) since 2021.

His research and work focus on the areas of sustainability (ESG), integrated ESGRC management systems, manager liability, governance, risk and compliance management, integrated human workflow management systems and digitalization, as well as contract, product liability, restructuring and insolvency law, labor law and human resources management.

Prof. Dr. Scherer is a partner and managing director of Governance-Solutions GmbH in the field of applied research and solutions/tools in the areas of ESG/GRC, digitalization, and integrated workflow management systems, and serves on the supervisory boards of various companies and foundations.

www.scherer-grc.net

LinkedIn: Prof. Dr. Josef Scherer
The author regularly publishes current judgments, laws, articles, etc. on ESGRC topics via LinkedIn.