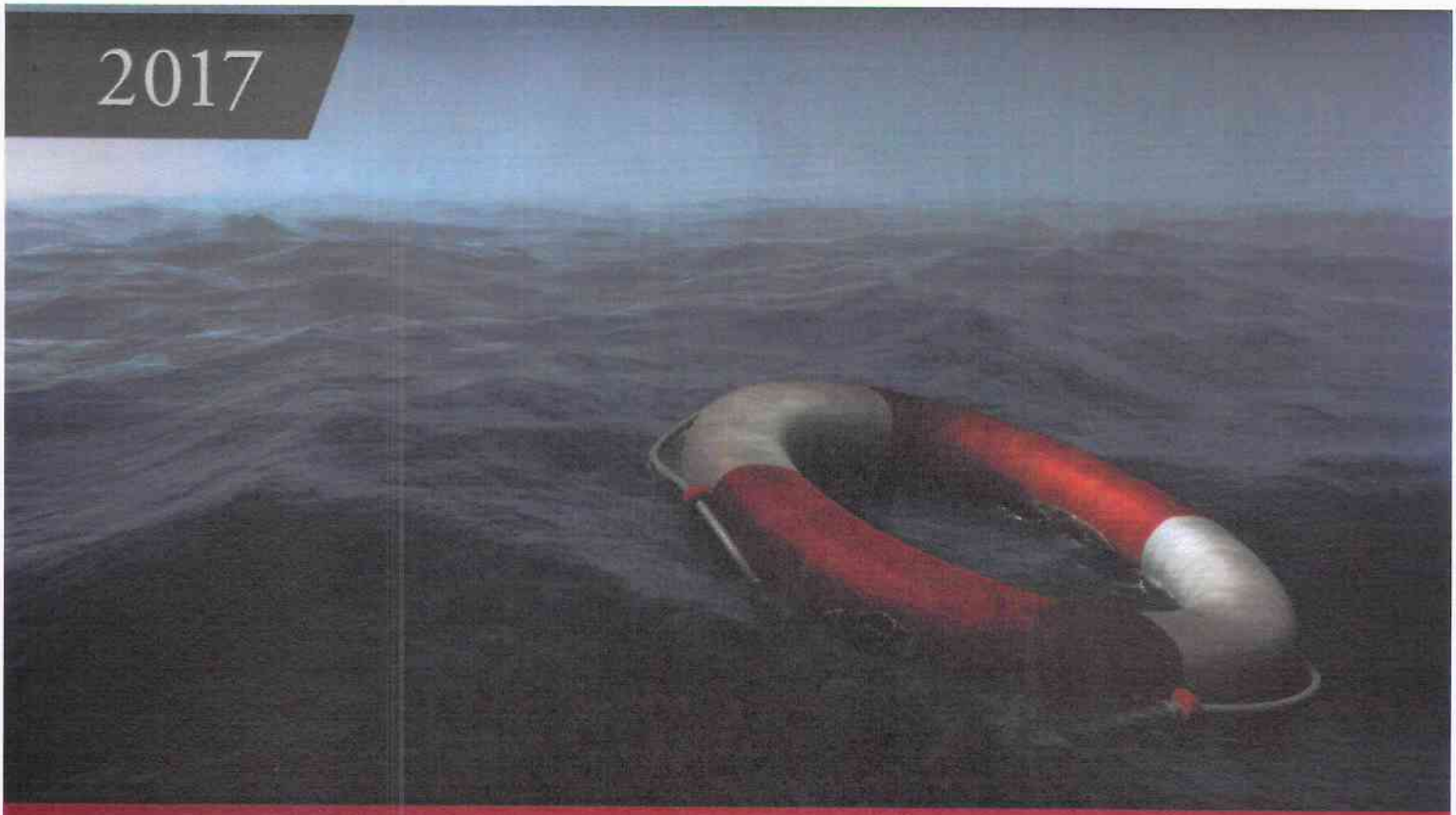
2017



Jahrbuch
Yearbook

FIRM
Frankfurter Institut für
Risikomanagement und Regulierung

The world(s) of monitoring: Huge potential for effectiveness, efficiency and value contributions in governance, risk & compliance (GRC)

Josef Scherer

It is possible to arrange different Monitoring Systems as stand-alone systems. However, this represents a novel approach of an integrated Monitoring System. This has proved in theory and practice to be coherent and suitable to network the multiple corporate functions, such as governance, risk and compliance management, internal controlling and monitoring system, revision etc., so as to avoid redundancies and island solutions and to achieve considerable synergies.

The objective of this "universal" standard "monitoring system" (download: www.gmrc.de) is to show that most of the standard works are built around a „common denominator", although they may differ in their structure and formulations.

In business practice, there are a wide variety of internal and external inspection / monitoring / audit / compliance assessment functions:

- 1st line of defense: Employees and colleagues, managers, board/ senior managers.
- 2nd line of defense: Controlling, ICS, risk management, compliance, quality management and other functions.
- 3rd line of defense: Auditing, assurance/internal investigation.
- 4th line of defense: Supervisory board, media, third parties (audits), public prosecutors, authorities, politicians, banks, courts (criminal, civil, administrative courts) etc.

Unfortunately, in practice these "monitors" do not act in concert but in parallel, even though they are essentially pursuing the same objectives: transparency of requirements for achieving business objectives, appropriate indicators tailored to these objectives and practised processes, supplemented with various mandatory and target requirements to guarantee the intended output. This is flanked by an appropriate and effective control and monitoring system.

The countless – redundant – activities identifiable in practice cost significant resources

Derived from the "Sarbanes Oxley Act" (SOX) and COSO, national and international auditors operate with their own auditing standards (for example IDW/IAS), some of which differentiate between concept, appropriateness, implementation, and effectiveness audits. For the "auditing world", for example, IDW EPS 981:2017 (Risk Management Systems) and IDW PS 341 (Early Risk Detection System) are relevant, but also COSO II:2004 (Enterprise Risk Management) and, in future, COSO II:2017 (Risk Aligned with Strategy and Performance).

For third party audits (for example certifications for customers on request or to use them for advertising) the international ISO world mainly offers effectiveness certifications / audits for management systems (whereby ISO 31000:2009 [the new version is due to appear in 2017/2018] cannot be certified, which is why ISO certifying bodies generally also use other standards [for example ONR 49000, which directly references ISO 31000:2009] for certification).

We should not forget the "world of auditing", for example standards issued by the "German Institute for Internal Auditing" (DIIR) in Germany or those issued by the "Institute of Internal Auditors" (IIA) globally. Applicable audit standards exist, such as DIIR no. 2:2014 (Audit of (Compliance) Risk Management).

The auditing world (but also supervisory authorities or public prosecutors) scrutinize the effectiveness, based on an appropriate concept and implementation.

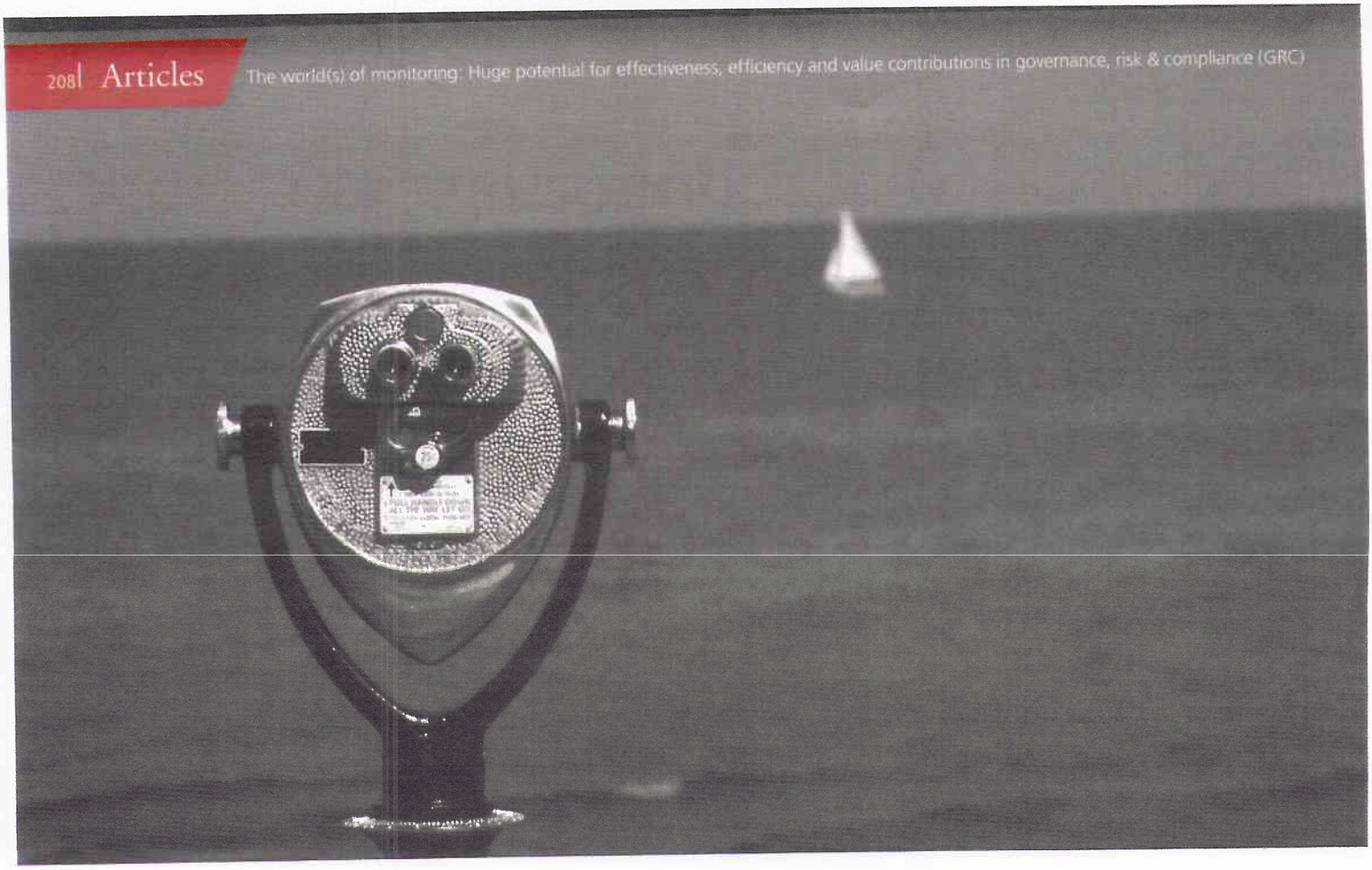
Harmonization seems to make sense here, with the objective of achieving "the best of both / three / four ... worlds". Using the example of the "needs of interested parties" component, which is required by almost every standard, we can clearly highlight the ease with which redundancies could be eliminated.

Because of the changed technological environment, with new communication possibilities guaranteeing increased presence and transparency especially for events that lead to huge reputation risks, the issue of "interested parties" is the subject of much greater focus in practice. This is also reflected in the requirements of "Industry 4.0" and the more recent standards (ISO/IDW/G20/OECD Principles of Corporate Governance etc.).

The first requirement of ISO 9001: 2015 in terms of "interested groups" in ISO 9001: 2015 (Quality Management System) is:

"4.2 Understanding the needs and expectations of interested parties

Due to their effect or potential effect on the organization's ability to consistently provide products and services that meet customer and applicable statutory and regulatory requirements, the organization shall determine: ***a) the interested parties that are relevant***



to the quality management system; b) the requirements of these interested parties *that are relevant to the quality management system."*

Comment: In my opinion, there is a lack of a requirement to evaluate particular needs (using appropriate risk management methods) and to implement required measures derived from them.

This first requirement specified in ISO 9001:2015 represents a mandatory requirement. As the "interested groups", such as authorities, regulators, customers etc., can exert a significant influence on the continuing existence of the company / organisation (for example by withdrawing orders, stopping production, imposing sanctions), it is one of the obligations of a conscientious entrepreneur (§§ 43 Limited Liability Companies Act (GmbHG), 93 Companies Act (AktG), 107 Companies Act (AktG), 347 German Commercial Code (HGB) etc.) to identify the relevant groups and their needs and, if necessary, to carry out the required measures.

Example: Resolving hygiene deficiencies (after repeated complaints by the supervisory authority) is merely reactive and may come too late and even trigger insolvency (case: bread factory in Freising). The correct approach is to know --in advance – what the authority's requirements of the company are and to meet them appropriately.

In the case mentioned, not only did the criminal division of the Landshut State Court press charges against the former Chief Executive, the public prosecutor also pressed charges against the former head of production and the quality officer.

Comparison (synopsis) with other standard texts that have the same requirements:
ISO 19600: 2014 (Compliance Management):
"4.2 Understanding the needs and expectations of interested parties (...)"

IDW PS 980: 2011 (Compliance Management System):
"5.4.1. Audit procedures for risk assessment (40) 5.4.1.1. Knowledge of the company's legal and economic environment (...)"

Similarly IDW PS 981: 2017 (Risk Management System):
"7.3.1 Gaining an understanding of the company and its legal and economic environment".

ONR 192050: 2013 (Compliance Management Systems):
No corresponding requirement is apparent here.

COSO I: 2013 (Internal Control): No corresponding explicit requirement is apparent here. However, there are requirements that at least indirectly relate to "interested groups":
"Assesses ***changes in the external environment. Principle 15:*** *The organisation* ***discusses with external parties*** *the functioning of the ICS."*

PAS 99: 2012 (Integrated Management System)
"4.2 Understanding the needs and expectations of interested parties"
ISO 9004: 2009 (Managing for the sustained success of an organisation)
"Interested parties, requirements and expectations"

DRS No. 20:2013 (Annual reporting) and **ISO 37001:2016 (Anti-corruption)** also require consideration of **"interested parties"**.

The situation is the same for all other components of the various standards. The requirement to perform a company analysis (organisation's internal context) appears in almost every standard. These redundant requirements, which can be represented as individual components, only have to be satisfied once(!).

Additional example: Every monitoring function (controlling / risk management / compliance / audits / internal auditing etc.) demands documented processes that meet various requirements

(effective, qualitative, legally sound, technically sound, efficient etc.): A single process audit can conduct the required target/actual comparison.

With the large number of monitoring measures outlined – in relation to the existence of "interested parties", company analysis or correct processes for example – there is a huge overlap and thus immense potential for savings, for example if a central function – coordinated with the other specialist areas – always performs the same checks (document / process / workflow checks / interviews etc.) and distributes the findings.

Ultimately, **monitoring and control measures should be automated as far as possible** to avoid tying up a disproportionate amount of personnel resources and to simultaneously avoid the susceptibility to error of human behaviour.

For example, **standard deviations** can easily be identified using automated mechanisms and then sent to appropriate employees for investigation of the causes and implementation of measures to prevent future errors.

A new, but certainly very sensible, approach that is already being practised by numerous companies is to set up a **data room containing the information that is normally required by all internal and external "interested parties"**, for example arranged by functional area or thematically. Associated – carefully selected – documents can also be provided. Authorised interested parties are then given exclusive **access privileges**, once they have signed corresponding non-disclosure agreements. For example, (positive) external audit results / certificates / indicators etc. can be provided. This would not reveal any business secrets, only positive PR.

The many redundant and analogous requirements / components from the various very similar current standards from the different "monitoring worlds" could also be combined wonderfully well into a **"Universal Combined Standard"** (on demand), with compliance attested by a **"Combined Certificate"**). *The Universal Standard Compliance Management System* standard with synoptic representation of the analogous requirements from ISO, COSO and IDW is available as a free download at www.gmrc.de.

Since the many monitoring functions use numerous redundant reference variables and standards, these can initially be combined from several individual standards for the same process and theme (for example for risk, compliance, quality management or personnel management systems) into a single N.N Universal Standard.

Likewise a combination of standards for different processes and themes into a "Meta Combined IMS Universal Standard" "on demand" (which individual management systems are to be merged?) is also possible, in terms of implementation but also in terms of auditing and certification.

Value contribution and value of an integrated management system

*"If a **high level of maturity** is reached in the various individual corporate functions / process areas / themes or in (corporate) governance more generally ("GRC as a bracket"), this **automatically** results in a **high level of sustainability, value contribution and fulfilment of obligations**. Thus, the objectives of companies, management and employees are very likely to be achieved, thus also leading to a **high level of goal attainment**."* [Scherer/Fruth 2016].

Achleitner also believes that "Corporate governance is an important value driver" [Achleitner 2015, p. 28]:

"Operational value creation will be the biggest challenge for companies (...) in the future. (...) In recent years, corporate governance in listed and public companies has often only been viewed from a monitoring perspective. The value creation aspect has been neglected. The key is better corporate decisions due to functioning and practised governance in the best commercial sense. (...) Good corporate governance practice will be a critical competitive factor in the future (...) and from investment practice we hear that there are cases where corporate governance accounts for two thirds of companies' increases in value. (...)"

Literature
Achleitner, P. [2015]: Corporate Governance als Werttreiber [Corporate Governance as a Value Driver], in: Handelsblatt, 30th June 2015, p. 28.
Scherer /, J./Fruth, K. (eds.) [2016]: Governance Management, Volume II (Standard & Audit), 2016.

Author
Prof. Dr. jur. Josef Scherer
International Institute of Governance, Management, Risk and Compliance Management at Deggendorf Institute of Technology and Management University of applied scienties and member of the FIRM advisory council