Janßen, Niklas

Article

Integrating sustainability in risk management and internal control systems: An empirical assessment of ESG reporting of German DAX40 firms

Junior Management Science (JUMS)

Provided in Cooperation with:
Junior Management Science e. V.

Suggested Citation: Janßen, Niklas (2025) : Integrating sustainability in risk management and internal control systems: An empirical assessment of ESG reporting of German DAX40 firms, Junior Management Science (JUMS), ISSN 2942-1861, Junior Management Science e. V., Planegg, Vol. 10, Iss. 4, pp. 858-875,
https://doi.org/10.5282/jums/v10i4pp858-875

This Version is available at:
https://hdl.handle.net/10419/334180

Online-Appendix

„Integrating Sustainability in Risk Management and Internal Control Systems: An Empirical Assessment of ESG Reporting of German DAX40 Firms“

Niklas Janßen

Leuphana University Lüneburg

Junior Management Science 10(4) (2025) 858-875

Appendix

Table B1. Overview of regulatory background.

Law	Norm	Related European directive	Amendment act	Year of first application	Material obligation	Selected aspects
			Focus on RMS and ICS			
			German legislation			
German Stock Corporation Act*	§ 91 Par. 2	-	KonTraG	FY 1999	Implementation	Implementation of an early warning risk system.
	§ 91 Par. 3	-	FISG	FY 2022	Implementation	Implementation of an appropriate and effective RMS and ICS within scope of activities and risk situation.
German Commercial Code*	§ 289 Par. 1; § 315 Par. 1[a b]	-	-	-	Reporting	Reporting on the underlaying assumptions relating to the assessed and explained material risks in the (group) management report.
	§ 289 Par. 4; § 315 Par. 4[a b]	2006/43/EG (2014/95/EU)[b]	BilMoG (CSR-RL-UG)[b]	FY 2010 (FY 2017)[b]	Reporting	Reporting on the main features of the RMS and ICS in relation to the (group) accounting process within (group) management report.
Supply Chain Due Diligence Act*	§ 4 Par. 1	-	-	FY 2024	Implementation	Implementation of an appropriate and effective RMS for compliance with due diligence obligations.
	§ 4 Par. 2	-	-	FY 2024	Implementation	Definition of who is responsible for the internal monitoring of the RMS.

	§ 5 Par. 1	-	-	FY 2024	Performance	Performing a risk analysis with regard to human rights and environmental risks within the scope of the own business activities and direct suppliers.
	§ 10 Par. 2	-	-	FY 2024	Reporting	Reporting on the risk measures from § 4 and 5. Reporting on how the company assesses the impact and effectiveness of these risk measures and what conclusions will be drawn.
German Corporate Governance Code**	Principle 4	-	-	FY 2022	Implementation	Implementation of an appropriate and effective ICS and RMS to responsibly manage risks within scope of activities. Performing internal monitoring of these systems.
	Principle 5	-	-	FY 2022	Implementation	Implementation of a CMS tailored to the organization's risk situation into the ICS and RMS in order to ensure compliance with laws and internal guidelines.
	Recommen-dation A.3	-	-	FY 2022	Implementation	Recommendation that the ICS and RMS shall also cover sustainable-related objectives, including processes and systems for collecting and processing respective data.
	Recommen-dation A.5	-	-	FY 2022	Reporting	Recommendation to describe the main characteristics of the ICS and RMS. Recommendation to provide a comment on the appropriateness and effectiveness of the ICS and RMS.
			European legislation			
European Sustainability	ESRS 2 IRO-1	-	-	FY 2024	Reporting	Reporting on the process used to identify, assess and prioritize and monitor risks. Reporting on the decision-making process and the

Reporting Standards*						related ICS procedures for the identification and assessment of risks. Reporting on the integration of the processes to identify, assess and manage risks into an overall RMS.
	ESRS 2 E1 Objective 20	-	-	FY 2024	Reporting	Disclosure Requirement related to ESRS 2 IRO-1. Reporting of processes to identify and assess material climate-related risks.
	ESRS 2 E2 Objective 11	-	-	FY 2024	Reporting	Disclosure Requirement related to ESRS 2 IRO-1. Reporting of processes to identify and assess material pollution-related risks.
	ESRS 2 E3 Objective 8	-	-	FY 2024	Reporting	Disclosure Requirement related to ESRS 2 IRO-1. Reporting of processes to identify and assess material water and marine resources-related risks.
	ESRS 2 E4 Objective 17	-	-	FY 2024	Reporting	Disclosure Requirement related to ESRS 2 IRO-1. Reporting of processes to identify and assess material biodiversity and ecosystem-related risks.
	ESRS 2 E5 Objective 11	-	-	FY 2024	Reporting	Disclosure Requirement related to ESRS 2 IRO-1. Reporting of processes to identify and assess material resource use and circular economy-related risks.
	ESRS 2 GOV-5			FY 2024	Reporting	Reporting on scope, main features and components of ICS and RMS in relation to sustainability reporting, including the assessment approach and risk prioritization methodology. Reporting on risk mitigation strategies and related controls. Reporting on integration of the findings of the ICS and RMS into internal functions.

Focus on ESG reports						
German legislation						
German Commercial Code*	§ 161	-	TransPuG	FY 2003	Reporting	Declaration of conformity with the German Corporate Governance Code.
	§ 289b; § 315b	2014/95/EU	CSR-RL-UG	FY 2017	Reporting	Obligation to provide a non-financial (group) statement.
	§ 289c; § 315c	2014/95/EU	CSR-RL-UG	FY 2017	Reporting	Content of the non-financial (group) statement.
	§ 290d	2014/95/EU	CSR-RL-UG	FY 2017	Reporting	Use of frameworks for non-financial (group) statement.
	§ 289e	2014/95/EU	CSR-RL-UG	FY 2017	Reporting	Omission of adverse information.
	§ 289f; § 315d	2014/95/EU	CSR-RL-UG	FY 2017	Reporting	Preparation of (group) corporate governance statement.
European legislation						
Corporate Sustainability Reporting Directive		Directive (EU) 2022/2464	Pending[d]	FY 2024	Reporting	-
Corporte Sustainability Due Diligence Directive		Directive (EU) 2024/1760	Pending[d]	FY 2028	Reporting	-

Note: This table presents an overview of the relevant regulatory environment for this paper. It is organized by relevant paragraphs related to the RMS and ICS, as well as to ESG reporting.

*Hard law. **Soft law.

[a] Paragraphs §289 par. 1 and §315 par. 1, as well as §289 par. 4 and §315 par. 4 contain the same provisions, whereby the paragraphs §315 refer to Groups.

[b] The BilMoG introduced § 289 Par. 5 GCC in 2009, according to which the key features of the internal control and risk management system about the accounting process must be described within the management report. With the CSR-RL-UG in 2017, paragraph 5 was relocated to paragraph 4 with the same legal text. For groups, the BilMoG introduced the corresponding paragraph § 315 Par. 2 no. 5 GCC for groups. The CSR-RL-UG in 2017, relocated paragraph 2 no. 5 to paragraph 4 with almost the same legal text.

[c] The presented sections in §315 relate to groups.

[d] At the time of writing this paper, there was no national law implementing these European Directives. For the CSRD, on 24 July 2024, the government draft of a law to implement the CSRD Directive was passed by the Federal Cabinet.

Table B2. Detailed sample.

#	Company	Industry sector	Type of analyzed report for 2022	Type of analyzed report for 2023
1	Adidas AG	Consumer	IR	IR
2	BASF SE	Chemicals*	IR	IR
3	Bayerische Motorenwerke AG	Automobile	IR	IR
4	Bayer AG	Chemicals*	AR, SR	AR, SR
5	Beiersdorf AG	Consumer	IR	IR
6	Brenntag SE	Chemicals*	IR	IR
7	Continental AG	Automobile	AR, SR	AR, SR
8	Covestro AG	Chemicals*	IR	IR
9	Daimler Truck Holding AG	Industrial*	IR	IR
10	Deutsche Post AG	Others	IR	IR
11	Deutsche Telekom AG	Others	AR, SR	AR, SR
12	Dr. Ing. h. c. F. Porsche AG	Automobile	IR	IR
13	E.ON SE	Utilities*	IR	IR
14	Fresenius SE & Co. KGaA	Pharma & Healthcare	IR	IR
15	Heidelberg Materials AG	Others*	IR	IR
16	Henkel AG & Co. KGaA	Consumer	AR, SR	AR, SR
17	Infineon Technologies AG	Others	AR, SR	AR, SR
18	Mercedes-Benz Group AG	Automobile	AR, SR	AR, SR
19	Merck KGaA	Pharma & Healthcare	AR, SR	AR, SR
20	MTU Aero Engines AG	Industrial*	AR, SR	AR, SR
21	Rheinmetall AG	Industrial*	AR, SR	AR, SR
22	RWE AG	Utilities*	AR, SRs	AR, SRs
23	SAP SE	Others	IR	IR
24	Sartorius AG	Pharma & Healthcare	AR, SR	AR, SR
25	Siemens AG	Industrial*	AR, SR	AR, SR
26	Siemens Energy AG	Industrial*	AR, SR	AR, SR
27	Symrise AG	Chemicals*	AR, SR	AR, SR
28	Volkswagen AG	Automobile	AR, SR	AR, SR
29	Zalando SE	Others	AR,SR	AR, SR

Table B3. General overview of the integrated disclosure index.

Categories and assessment criteria	Affected system	Analyzed report section	Derivation basis for index category: COSO ICIF component (principle)	Derivation basis for index category: COSO ERMF component (principle)	Derivation basis for index category: Regulatory environment	Maximum no. of points
			(1) General characteristics			***0-12***
1 General system environment						*4*
1.1 Commitment to sustainability	both	All parts	Control environment (1)	Governance & culture (3, 4)		1
1.2 Institutionalization of structures and authority	both	All parts	Control environment (3)	Governance & culture (2)		1
1.3 Commitment to competent human resources	both	All parts	Control environment (4)	Governance & culture (5)		1
1.4 Enforcement of individual accountability	both	All parts	Control environment (5)	Governance & culture (1)		1
2 Statement on system setup						*4*
2.1 Declaration of compliance with recommendation A.3 of the GCGC		CGS / risk & opp. report	Risk assessment (6)	Strategy & objective-setting (9)		1
2.2 Statement of integrating sustainability issues into the ERM	ERM	CGS / risk & opp. report	Risk assessment (6)	Strategy & objective-setting (9)		1
2.3 Statement of integrating sustainability issues into the ICS	ICS	CGS / risk & opp. report	Risk assessment (6)	Strategy & objective-setting (9)		1
2.4 Statement of integrating sustainability issues into the CMS	CMS	CGS / risk & opp. report	Risk assessment (6)	Strategy & objective-setting (9)		1
3 Specific system setup						*4*
3.1 Consideration of special, sustainability-related aspects of the business context, or sector	both	Management report	Risk assessment (6)	Strategy & objective-setting (6)		1

3.2 Definition and explanation of sustainability-related risk appetite	ERM	Management report	Risk assessment (6)	Strategy & objective-setting (7)		1
3.3 Consideration of (un)intended misuse	both	Management report	Risk assessment (8)	Strategy & objective-setting (7)		1
3.4 Application of specific management systems	both	Management report	Risk assessment (8)	Strategy & objective-setting (7)		1
			(2) Performance on environmental issues			***0-25***
4 Performance I: Climate Change					*ESRS E1****	*5*
4.1 General statement of integration into RMS	ERM	All parts	Risk assessment (6)	Strategy & objective-setting (9)		1
4.2 Process of risk identification, assessment and prioritization	ERM	All parts	Risk assessment (7)	Performance (10, 11, 12)		1
4.3 Process of risk mitigation and response	ERM	All parts	Risk assessment (7)	Performance (13)		1
4.4 Application of technology	both	All parts	Control activities (11)	Information, communication & reporting (18)		1
4.5 Relevance and quality of data	both	All parts	Information and communication (13)	Information, communication & reporting (18)		1
5 Performance II: Pollution					*ESRS E2****	*5*
5.1 General statement of integration into RMS	ERM	All parts	Risk assessment (6)	Strategy & objective-setting (9)		1
5.2 Process of risk identification, assessment and prioritization	ERM	All parts	Risk assessment (7)	Performance (10, 11, 12)		1
5.3 Process of risk mitigation and response	ERM	All parts	Risk assessment (7)	Performance (13)		1

5.4 Application of technology	both	All parts	Control activities (11)	Information, communication & reporting (18)		1
5.5 Relevance and quality of data	both	All parts	Information and communication (13)	Information, communication & reporting (18)		1
6 Performance III: Water and marine resources					*ESRS E3****	*5*
6.1 General statement of integration into RMS	ERM	All parts	Risk assessment (6)	Strategy & objective-setting (9)		1
6.2 Process of risk identification, assessment and prioritization	ERM	All parts	Risk assessment (7)	Performance (10, 11, 12)		1
6.3 Process of risk mitigation and response	ERM	All parts	Risk assessment (7)	Performance (13)		1
6.4 Application of technology	both	All parts	Control activities (11)	Information, communication & reporting (18)		1
6.5 Relevance and quality of data	both	All parts	Principle 13	Information, communication & reporting (18)		1
7 Performance IV: Biodiversity and ecosystems					*ESRS E4****	*5*
7.1 General statement of integration into RMS	ERM	All parts	Risk assessment (6)	Strategy & objective-setting (9)		1
7.2 Process of risk identification, assessment and prioritization	ERM	All parts	Risk assessment (7)	Performance (10, 11, 12)		1
7.3 Process of risk mitigation and response	ERM	All parts	Risk assessment (7)	Performance (13)		1

7.4 Application of technology	both	All parts	Control activities (11)	Information, communication & reporting (18)		1
7.5 Relevance and quality of data	both	All parts	Information and communication (13)	Information, communication & reporting (18)		1
8 Performance V: Resource use and circular economy					*ESRS E5****	*5*
8.1 General statement of integration into RMS	ERM	All parts	Risk assessment (6)	Strategy & objective-setting (9)		1
8.2 Process of risk identification, assessment and prioritization	ERM	All parts	Risk assessment (7)	Performance (10, 11, 12)		1
8.3 Process of risk mitigation and response	ERM	All parts	Risk assessment (7)	Performance (13)		1
8.4 Application of technology	both	All parts	Control activities (11)	Information, communication & reporting (18)		1
8.5 Relevance and quality of data	both	All parts	Information and communication (13)	Information, communication & reporting (18)		1
			(3) Monitoring			***0-8***
9 Internal oversight						*5*
9.1 Identification and analysis of sustainability-related changes and trends affecting the systems	both	Management report	Risk assessment (9)	Review and revision (15)		1
9.2 Conducting internal audit with focus on sustainability	both	Management report	Monitoring activities (16)	Review and revision (16)		1
9.3 Evaluations and improvement of the systems	both	Management report	Monitoring activities (16)	Review and revision (17)		1

9.4 Establishment and communication of internal CSR-related policies	both	Management report	Control activities / information & communication (12 / 14)	Information, communication & reporting (18, 19)		1
9.5 “Comment on appropriateness and effectiveness” with regard to sustainability	both	Management report	Monitoring activities (17)	Information, communication & reporting (20)	A.5 GCGC**	1
10 External oversight						*3*
10.1 Reports on external, voluntary audit of the sustainability-related RMS	ERM	Auditors report	Monitoring activities (16, 17)	Review and revision (16)	IDW PS 981**	1
10.2 Reports on external, voluntary audit of the sustainability-related ICS	ICS	Auditors report	Monitoring activities (16, 17)	Review and revision (16)	IDW PS 982**	1
10.3 Reports on external, voluntary audit of the sustainability-related CMS	CMS	Auditors report	Monitoring activities (16, 17)	Review and revision (16)	IDW PS 983**	1

Note: Abbreviations: CGS = Corporate Governance Statement. ICIF = Internal Control Integrated Framework (see COSO, 2013). ERMF = Enterprise Risk Management Integrating with Strategy and Performance Framework (see COSO, 2017).

*Hard law. **Soft law; voluntary, non-statutory standard. ***Future regulation.

Table B4. Detailed overview of the integrated disclosure index.

No.		Derivation basis for each assessment criterion and explanation of deviations.	Point Range
		(1) General characteristics	***0-12***
1		*General system environment*	*0-4*
	1.1	<u>*Commitment to sustainability*</u> "The organization demonstrates a commitment to integrity and ethical values." (ICIF 2013, Principle 1). "The organization defines the desired behaviors that characterize the entity's desired culture." (ERMF 2017, Principle 3). "The organization demonstrates a commitment to the entity's core values." (ERMF 2017, Principle 4). 0 = No indication of commitment to sustainability. 1 = Indication for commitment. For example, sustainability is mentioned as a core strategy element, or there is a commitment to the Science Based Targets initiative.	0-1
	1.2	<u>*Institutionalization of structures and authority for sustainability objectives*</u> "Management establishes […] structures, reporting lines […] in the pursuit of objectives." (ICIF 2013, Principle 3). "The organization establishes operating structures in the pursuit of strategy and business objectives." (ERMF 2017, Principle 2). 0 = No indication of the institutionalization of structures and authorities with regard to the pursuit of the achievement of sustainability objectives. 1 = Indication for institutionalization. For example, structures such as a sustainability committee or the existence of a chief sustainability officer are described.	0-1
	1.3	<u>*Commitment to competent human resources*</u> "The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives." (ICIF 2013, Principle 4). "The organization is committed to building human capital in alignment with the strategy and business objectives." (ERMF 2017, Principle 5). 0 = No indication of commitment to competent human resources. 1 = Indication for commitment. For example, there is training in the area of risk management or risk compliance management.	0-1
	1.4	<u>*Enforcement of individual accountability*</u> "The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives. (ICIF-2013, Principle 5). "The board of directors […] carries out governance responsibilities to support management in achieving strategy and business objectives." (ERMF 2017, Principle 1).	0-1

0 = No indication of enforcement of individual accountability for risk management or internal control.
1 = Indication for enforcement of individual accountability. For example, there is a clear description of the person responsible for risk management or internal control processes.

2	*Statement on system setup*	*0-4*

2.1 <u>*Declaration of compliance with recommendation A.3 of the GCGC*</u> 0-1

"The internal control system and the risk management system shall also cover sustainability-related objectives, unless required by law anyway. This shall include processes and systems for collecting and processing sustainability-related data." (GCGC, Recommendation A.3). Declaration on the Corporate Governance Code pursuant to § 161 GSCA.

0 = Declared deviation from the recommendation.
1 = No declared deviation, or a statement of conformity.

2.2 <u>*Statement of integrating sustainability issues into the ERM*</u> 0-1

"The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives." (ICIF 2013, Principle 6).
"The organization considers risk while establishing the business objectives at various levels that align and support strategy." (ERMF 2017; Principle 9).
"The internal control system and the risk management system shall also cover sustainability-related objectives, unless required by law anyway. This shall include processes and systems for collecting and processing sustainability-related data." (GCGC, Recommendation A.3)

0 = No indication of integration of sustainability issues into the ERM.
1 = Indication for the integration. For example, integration of sustainability issues is explicitly mentioned.

2.3 <u>*Statement of integrating sustainability issues into the ICS*</u> 0-1

"The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives." (ICIF 2013, Principle 6).
"The organization considers risk while establishing the business objectives at various levels that align and support strategy." (ERMF 2017; Principle 9).
"The internal control system and the risk management system shall also cover sustainability-related objectives, unless required by law anyway. This shall include processes and systems for collecting and processing sustainability-related data." (GCGC, Recommendation A.3)

0 = No indication of integration of sustainability issues into the ICS.
1 = Indication for the integration. For example, integration of sustainability issues is explicitly mentioned.

2.4	*Statement of integrating sustainability issues into the CMS* "The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives." (ICIF 2013, Principle 6). "The organization considers risk while establishing the business objectives at various levels that align and support strategy." (ERMF 2017; Principle 9). "The internal control system and risk management system comprise a compliance management system aligned to the enterprise's risk situation." (GCGC, Principle 5) "The internal control system and the risk management system shall also cover sustainability-related objectives, unless required by law anyway. This shall include processes and systems for collecting and processing sustainability-related data." (GCGC, Recommendation A.3) 0 = No indication of integration of sustainability issues into the CMS. 1 = Indication for the integration. For example, integration of sustainability issues is explicitly mentioned.	0-1
3	*Specific system setup*	*0-4*
3.1	*Consideration of special, sustainability-related aspects of the business context, or sector* "The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives." (ICIF 2013, Principle 6). "The organization considers potential effects of business context on risk profile." (ERMF 2017; Principle 6). 0 = No indication of consideration of special, sustainability-related aspects of the business context, or sector. 1 = Indication for the consideration. For example, there is a clear statement in the reference to sector-specific characteristics and sustainability issues.	0-1
3.2	*Definition and explanation of sustainability-related risk appetite* "The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives." (ICIF 2013, Principle 6). "The organization defines risk appetite in the context of creating, preserving, and realizing value." (ERMF 2017; Principle 7). 0 = No indication of definition and explanation of sustainability-related risk appetite. 1 = Indication for the definition and explanation. For example, there is a clear explanation of the sustainability-related risk appetite.	0-1
3.3	*Consideration of (un)intended misuse on environmental issues* "The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives." (ICIF 2013, Principle 6).	0-1

"The organization defines risk appetite in the context of creating, preserving, and realizing value." (ERMF 2017; Principle 7).

0 = No indication of consideration of (un)intended misuse on environmental issues.
1 = Indication for the consideration. For example, there is a clear statement on dealing with fraud in environmental matters within the organization.

3.4 *Application of specific management systems* 0-1

"The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives." (ICIF 2013, Principle 6).
"The organization defines risk appetite in the context of creating, preserving, and realizing value." (ERMF 2017; Principle 7).

0 = No indication of the application of specific management systems.
1 = Indication for the application. For example, there is a clear statement on the integration of an ISO 140001 environmental management system.

(2) Performance on environmental issues ***0-25***

Note. Only category 4 is shown with all respective assessment criteria as an example in this overview. The same six assessment criteria apply to categories 5 to 8, considering the different sustainability issues.

4	*Performance I: Climate Change* *Note. The main objective of the ESRS E1 is to gain an understanding of how the company affects climate change. This paper focuses in particular on the aspect of greenhouse gases.*	0-5

4.1 Statement of integration into ERM / ICS

0 = No indication for a statement of the integration of climate change into the RMS/ICS.
1 = Indication for the integration. For example, there is a clear statement that risks associated with climate change are integrated into the ERM/ICS.

4.2 *Process of risk identification, assessment and prioritization* 0-1

"The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed." (ICIF 2013, Principle 7).
"The organization identifies risk that impacts the performance of strategy and business objectives." (ERMF 2017; Principle 10)
"The organization assesses the severity of risk." (ERMF 2017; Principle 11).
"The organization prioritizes risks as a basis for selecting responses to risks." (ERMF 2017; Principle 12).

	0 = No indication of a process for risk identification, assessment and prioritization. 1 = Indication for a respective process. For example, there is a clear description of risks identification in connection with climate change (e.g. GHG emissions).	
4.3	<u>*Process of risk mitigation and response*</u> *Note:* "The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed." (ICIF 2013, Principle 7). "The organization identifies and selects risk responses." (ERMF 2017; Principle 13). 0 = No indication of a process for risk mitigation and response. 1 = Indication for a respective process. For example, there is a clear description of risk mitigation in connection with climate change (e.g. GHG emissions reduction).	0-1
4.4	<u>*Application of technology*</u> *Note:* "The organization selects and develops general control activities over technology to support the achievement of objectives." (ICIF 2013, Principle 11); "The organization leverages the entity's information and technology systems to support enterprise risk management." (ERMF 2017; Principle 18). 0 = No indication of the application of technology. 1 = Indication for the application. For example, there is a description of applied tools used for risk identification.	0-1
4.5	<u>*Relevance and quality of data*</u> *Note:* "The organization obtains or generates and uses relevant, quality information to support the functioning of internal control." (ICIF 2013, Principle 12); "The organization leverages the entity's information and technology systems to support enterprise risk management." (ERMF 2017; Principle 18). 0 = No indication for a statement on the relevance and quality of the data in the context of risk management and internal control processes. 1 = Indication for relevance and quality. For example, there is a statement regarding the quality of the data collected as part of risk management.	0-1
	Performance II: Pollution *Note. The main objective of the ESRS E2 is to gain an understanding of how the organization affects pollution of the air, as well as water and soil.*	0-5
	Performance III: Water and marine resources *Note. The main objective of the ESRS E3 is to gain an understanding of how the organization affects water and marine resources, for example the reduction of water consumption.*	0-5

	Performance IV: Biodiversity and ecosystems *Note. The main objective of the ESRS E4 is to gain an understanding of how the organization affects biodiversity and ecosystems.*	0-5
	Performance V: Resource use and circular economy *Note. The main objective of the ESRS E4 is to gain an understanding of how the organization deals with resources and circular economy.*	0-5
	(3) Monitoring	***0-8***
9	*Internal oversight*	0-5

9.1 *Identification and analysis of sustainability-related changes and trends affecting the systems* — 0-1

Note: "The organization identifies and assesses changes that could significantly impact the system of internal control." (ICIF 2013, Principle 9);
"The organization identifies and assesses changes that may substantially affect strategy and business objectives." (ERMF 2017; Principle 15).

0 = No indication of the consideration sustainability-related changes and trends that affect the systems.
1 = Indication for the consideration. For example, there is a statement on how sustainability-related changes affects the systems.

9.2 *Conducting internal audit with focus on sustainability* — 0-1

Note: "The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning." (ICIF 2013, Principle 16);
"The organization reviews entity performance and considers risk." (ERMF 2017; Principle 16).

0 = No indication for conducting internal audit with focus on sustainability issues.
1 = Indication for conducting a respective internal audit. For example, there is a statement that the internal audit also focuses on sustainability issues.

9.3 *Evaluations and improvement of the systems* — 0-1

Note: "The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning." (ICIF 2013, Principle 16);
"The organization pursues improvement of enterprise risk management." (ERMF 2017; Principle 17).

0 = No indication of evaluations and improvement of the systems with regard to sustainability issues.
1 = Indication for evaluations and improvement of the systems. For example, there is a description of conducted evaluations.

9.4 *Establishment and communication of internal CSR-related policies* 0-1

Note: “The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.” (ICIF 2013, Principle 12);
“The organization pursues improvement of enterprise risk management.” (ICIF 2013, Principle 14); “The organization leverages the entity’s information and technology systems to support enterprise risk management.” (ERMF 2017; Principle 18);
“The organization uses communication channels to support enterprise risk management.” (ERMF 2017; Principle 19).

0 = No indication of the establishment and communication of internal CSR-related policies with regard to the systems.
1 = Indication for the establishment and communication. For example, there is a statement that internal risk management policies include sustainability issues.

9.5 *“Comment on appropriateness and effectiveness” with regard to sustainability* 0-1

Note: “The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.” (ICIF 2013, Principle 17).
“The organization reports on risk, culture, and performance at multiple levels and across the entity.” (ERMF 2017; Principle 20).
This category is mainly based on the recommendation A.5 of the German Corporate Governance Code: “The management report shall […] provide comment upon the appropriateness and effectiveness […].”

0 = No consideration of sustainability issues in the statement on the appropriateness and effectiveness of the ERM and ICS.
1 = Consideration of sustainability issues within the statement.

10	*External oversight*	0-3

10.1 *Reports on external, voluntary audit of the sustainability-related ERM* 0-1

Note: “The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.” (ICIF 2013, Principle 16).
“The organization reviews entity performance and considers risk. (ICIF 2013, Principle 16).
The organization conducts external voluntary audits of its ERM to IDW PS 981. External auditors can conduct external audits with sufficient assurance regarding appropriateness in accordance with IDW PS 980 (ERM), 981 (ICS), and 982 (CMS) (IDW, 2023).

0 = No indication of an external, voluntary audit of the sustainability-related ERM.

1 = Indication or auditors report on a voluntary audit of the sustainability-related ERM.

10.2 *Reports on external, voluntary audit of the sustainability-related ICS* 0-1

Note: "The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning." (ICIF 2013, Principle 16).
"The organization reviews entity performance and considers risk." (ICIF 2013, Principle 16).
The organization conducts external voluntary audits of its ICS to IDW PS 982. External auditors can conduct external audits with sufficient assurance regarding appropriateness in accordance with IDW PS 980 (ERM), 981 (ICS), and 982 (CMS) (IDW, 2023).

0 = No indication of an external, voluntary audit of the sustainability-related ICS.
1 = Indication or auditors report on a voluntary audit of the sustainability-related ICS.

10.3 *Reports on external, voluntary audit of the sustainability-related CMS* 0-1

Note: "The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning." (ICIF 2013, Principle 16).
"The organization reviews entity performance and considers risk." (ICIF 2013, Principle 16).
The organization conducts external voluntary audits of its ICS to IDW PS 983. External auditors can conduct external audits with sufficient assurance regarding appropriateness in accordance with IDW PS 980 (ERM), 981 (ICS), and 982 (CMS) (IDW, 2023).

0 = No indication of an external, voluntary audit of the sustainability-related CMS.
1 = Indication or auditors report on a voluntary audit of the sustainability-related CMS.

Note. This disclosure index is mainly derived on the basis of the Internal Control – Integrated Framework (ICIF) of 2013 (see COSO, 2013) and on the Enterprise Risk Management Integrating with Strategy and Performance Framework (ERMF) (see COSO, 2017). The assessment criteria are mainly based on the principles from the frameworks. In individual cases, additional explanations (e.g. Point Of Focus) were used to derive the criteria. For reasons of clarity, these are not listed here.
The relevant sources, where indicated, are the following. ICIF = COSO (2013). ERMF = COSO (2017).

Table B5. Detailed scoring across all assessment criteria.

Assessment criterion	2023 Mean	2023 Median	2023 $Points_{Max}$	2023 $Points_{Min}$	2022 Mean	2022 Median	2022 $Points_{Max}$	2022 $Points_{Min}$
Cat. 1	*3.79*	*4*	*4*	*3*	*3.97*	*4*	*4*	*3*
1.1	1.0	1	—	—	1.0	1	—	—
1.2	1.0	1	—	—	1.0	1	—	—
1.3	0.83	1	—	—	0.97	1	—	—
1.4	0.97	1	—	—	1.0	1	—	—
Cat. 2	*2.90*	*3*	*4*	*2*	*2.69*	*3*	*4*	*1*
2.1	1.0	1	—	—	0.90	1	—	—
2.2	0.90	1	—	—	0.86	1	—	—
2.3	0.72	1	—	—	0.62	1	—	—
2.4	0.28	0	—	—	0.31	0	—	—
Cat. 3	*1.66*	*2*	*3*	*0*	*1.59*	*2*	*3*	*0*
3.1	0.48	0	—	—	0.45	0	—	—
3.2	0.10	0	—	—	0.07	0	—	—
3.3	0.14	0	—	—	0.14	0	—	—
3.4	0.93	1	—	—	0.93	1	—	—
Cat. 4	*3.34*	*3*	*5*	*2*	*3.14*	*3*	*5*	*2*
4.1	0.41	0	—	—	0.38	0	—	—
4.2	1.0	1	—	—	1.0	1	—	—
4.3	1.0	1	—	—	1.0	1	—	—
4.4	0.45	0	—	—	0.31	0	—	—
4.5	0.48	0	—	—	0.45	0	—	—
Cat. 5	*1.24*	*1*	*4*	*0*	*1.24*	*1*	*4*	*0*
5.1	0.07	0	—	—	0.03	0	—	—
5.2	0.21	0	—	—	0.17	0	—	—
5.3	0.86	1	—	—	0.86	1	—	—
5.4	0.03	0	—	—	0.07	0	—	—
5.5	0.07	0	—	—	0.10	0	—	—
Cat. 6	*2.66*	*3*	*5*	*0*	*2.38*	*2*	*5*	*0*
6.1	0.17	0	—	—	0.07	0	—	—
6.2	0.86	1	—	—	0.76	1	—	—
6.3	0.90	1	—	—	0.90	1	—	—
6.4	0.45	0	—	—	0.45	0	—	—
6.5	0.28	0	—	—	0.28	0	—	—
Cat. 7	*1.83*	*2*	*5*	*0*	*1.55*	*1*	*5*	*0*
7.1	0.14	0	—	—	0.07	0	—	—
7.2	0.45	0	—	—	0.38	0	—	—
7.3	0.83	1	—	—	0.79	1	—	—
7.4	0.31	0	—	—	0.21	0	—	—
7.5	0.10	0	—	—	0.10	0	—	—
Cat. 8	*1.97*	*2*	*4*	*0*	*1.62*	*1*	*4*	*0*
8.1	0.10	0	—	—	0.03	0	—	—
8.2	0.48	0	—	—	0.41	0	—	—
8.3	0.93	0	—	—	0.86	0	—	—
8.4	0.17	0	—	—	0.10	0	—	—

8.5	0.28	0	—	—	0.21	0	—	—
Cat. 9	*0.79*	*0*	*4*	*0*	*0.55*	*0*	*4*	*0*
9.1	0.03	0	—	—	0.00	0	—	—
9.2	0.21	0	—	—	0.10	0	—	—
9.3	0.38	0	—	—	0.28	0	—	—
9.4	0.07	0	—	—	0.07	0	—	—
9.5	0.10	0	—	—	0.10	0	—	—
Cat. 10	*0.00*	*0*	*0*	*0*	*0.00*	*0*	*0*	*0*
10.1	0.00	0	—	—	0.00	0	—	—
10.2	0.00	0	—	—	0.00	0	—	—
10.3	0.00	0	—	—	0.00	0	—	—

Note. $\text{Score}_{\text{Max}}$ = Maximum score achieved. $\text{Score}_{\text{Min}}$ = Minimum score achieved.