



# DIIR

## ESG Audit Guide

Assessing the management of sustainability risks in financial services institutions

Prepared by the Banking Working Groups of the  
DIIR - Deutsches Institut für Interne Revision e.V.

Status: 8.12.2022

## Preamble

The ESG Audit Guide was developed by a group of expert auditors from German banks who are involved in various working groups of the DIIR - Deutsches Institut für Interne Revision e.V. (IIA Germany). Taking up our suggestion to create such a guideline, a group of authors was formed, which put the project into practice with great commitment within a short period of time. We owe a great debt of gratitude to the authors.

The guideline is the result not only of an analysis of isolated existing regulations and consultations, but also of intensive discussions. This is because the topic of sustainability is a young field of auditing for which ready-made audit catalogues and checklists cannot be found at the present time, but for which - on the contrary - fundamental requirements and benchmarks are only in the process of being developed and are also still subject to major changes.

The present work has created the basis for approaching the audit object from different directions. The modular structure allows adaptation to the respective circumstances and different focal points. It is becoming very clear that the audit object will expand in the coming years. The Audit Guide will develop accordingly and may become established as a standard.

On behalf of the Executive Board of DIIR - Deutsches Institut für Interne Revision e.V.

Andrea Bracht  
Member of the DIIR Executive Board

Dr. Stephan Lauer  
Member of the DIIR Executive Board

## Foreword

The transformation of the economy currently taking place through the shift in the field of sustainability in the areas of environmental, social, and governance (ESG) has far-reaching implications for the financial sector. The financial risk potential, which is inherent in change, is to be identified, assessed, managed, monitored, and made transparent by means of disclosure regulations in accordance with the requirements of German and European supervisory authorities. Among other things, Internal Auditing can create added value in the company through an ex ante-oriented audit and identify implementation risks, deficiencies, and potential for improvement at an early stage.

This DIIR ESG Audit Guide intends to support the internal auditors of financial services institutions designing a structured and target-oriented readiness assessment and evaluating the management of sustainability risks. In line with the modular nature of the audit guide, non-binding questions to guide the audit are presented in the sense of a good practice approach, regardless of whether this is implemented in the form of regular audits, project monitoring or special audits. In this way, modules can be flexibly selected for each type of audit (product, process or governance audit) and for different audit approaches. The categorization of audit questions as **basic questions (B)** and **in-depth questions (D)** intends to take the proportionality principle into account. In principle, the guide can serve as a compendium for all internal audit functions, regardless of the degree of regulation of the organization's operating environment.

The DIIR ESG Audit Guide makes an attempt to map the requirements and expectations of banking supervision with regard to risk management and disclosure and is based in particular on the BaFin bulletin on dealing with sustainability risks (December 20, 2019, last amended on October 1, 2021), the BaFin survey on sustainability risks (October 14, 2021), and the ECB guidance on climate and environmental risks (May 2020).

The DIIR ESG Audit Guide consists of the following chapters

1. Responsible corporate governance and strategies,
2. Business organization and
3. Risk management.

In some cases, there are deliberate redundancies in the individual audit objects in order to enable appropriate partial and cross-sectional audits in different areas.

The authors welcome feedback on the manageability of the audit guide. This is intended to support the ongoing quality assurance and further development of the audit guide in the future. The feedback questions can be found in Section 4 (Appendices) and in an Excel document that is provided along with the audit guide.

In addition, the authors make a proposal for self-assessment with regard to the individual audit fields. This also forms the basis for a planned anonymized DIIR benchmarking between participating organizations. The template for the self-assessment can also be found in the Excel document that is provided along with the audit guide.

## Content

1	Responsible corporate governance and strategies.....	6
2	Business organization.....	11
3	Risk management.....	16
4	Attachments.....	25
4.1	Feedback questionnaire.....	25
4.2	Legal sources.....	26
4.3	Definitions.....	27

## 1 Responsible corporate governance and strategies

	<b>Audit field and guiding questions</b>	<b>Note</b>	<b>Possible audit procedures</b>
	<b>Corporate Governance</b>		
1 B	Are the roles and responsibilities clearly defined and has there been a clear allocation and division of duties and tasks with regard to strategy responsibility incl. process responsibility among the executive board and management?	BaFin bulletin 4.1, 4.2 ECB Guide, Expectation 3.1	Review of written rules and regulations
2 B	Is there adequate participation and involvement of senior management in the definition and management of sustainability risks?	BaFin Fact Sheet 4.2 ECB Guide, Expectation 3.3	Review of written rules and regulations, minutes of meetings, project control documents
3 B	Are the procedures adequate to ensure that members of management have adequate knowledge and skills to assess sustainability risks?	BaFin Leaflet 4.2 ECB Guideline, Expectation 3.2	Review of rules and regulations, meeting minutes, project control documents, committee training planning
4 B	How does management demonstrate "leading by example" (tone from the top)?  Is there a commitment to sustainability in the bank?	BaFin bulletin 4.4	Review organizational guidelines  Review of in-house announcements, publications, press releases

5 B	How is the successful management of sustainability risks or compliance with strategic sustainability goals aligned with executive compensation?	BaFin Fact Sheet 4.4 ECB Guide, Expectation 4.3	Review organizational guidelines, review assessment criteria of compensation systems
<b>Business Strategy</b>			
6 B	How is the handling (measures) of sustainability risks regulated? (Own strategy or as part of an existing strategy)	BaFin bulletin 3.1.1 ECB Guide, Expectation 1.2, 2	Review of strategies (business, risk strategy) Comparison with sustainability report (non-financial reports)
7 D	How is it ensured that different areas of the company are involved as fully as possible in integrating sustainability risks into the business or risk strategy?	BaFin bulletin 3.1.1	Review of strategies (business, risk strategy) Comparison with sustainability report (non-financial reports)
8 B	Is it regulated in which time frame the implementation of the strategic goals for sustainability risks should take place?	BaFin bulletin 3.1.1	Review of strategies (business, risk strategy) Comparison with sustainability report (non-financial reports) Review of project documents

9 B	Does the company follow external sustainability standards or recommendations? If yes, is this reflected in the company's own strategies and organizational guidelines and is it sufficiently comprehensible? (Are areas classified as sustainable/non-sustainable? )	<p>BaFin bulletin 3.1.2</p> <p>Principles for Responsible Banking, Principles for Responsible Investment, Principles for Sustainable Insurance</p> <p>Recommendations of the Task Force on Climate-related Financial Disclosures</p> <p>German Sustainability Code</p> <p>SD-KPI Standard 2016-2021</p> <p>Berlin CSR Consensus on Corporate Responsibility in Supply and Value Chains</p>	<p>Review strategies and organizational policies</p> <p>Analysis of decision protocols</p>
10 B	Which business areas are affected by physical risks and to what extent, and what are the (long-term) effects?	<p>BaFin bulletin 3.2.1</p> <p>ECB Guide, Expectation 1.1, 1.2</p>	Review of the business segment analyses
11 B	Which business areas are affected by transitory risks and to what extent, and what are the (long-term) effects?	<p>BaFin bulletin 3.2.2</p> <p>ECB Guide, Expectation 1.1, 1.2</p>	Review of the business segment analyses
12 D	How does the company deal with sustainability requirements for third parties (e.g., customers, suppliers, stakeholders)?	BaFin bulletin 3.2.2	Retrace the decision (e.g., committee minutes) as to whether sustainability requirements should be imposed on third parties. Is this documented?



13 B	How does the company take into account the sustainability awareness of stakeholders or its impact on the (future) business model?	BaFin bulletin 3.2.3	Review of processes for analyzing the business model with regard to the consideration of potential need for change
14 D	Are attempts made to put investment objects or contractual partners on a sustainable course via the exercise of voting rights or dialog with company management or industry representatives?	BaFin bulletin 6.2.6, 6.3.4.1, 6.3.4.2  Exercise of voting rights, especially for KVGs	Review of investment strategy  Review of banking book strategy/treasury strategy
15 B	Has the company decided to offer sustainable products and specified this in the strategies?	BaFin bulletin 3.2.3	Verification of internal/external attestations for products  Review NPP/product catalog
16 B	Is there an impact analysis of sustainability risks on regulatory capital ratios?	BaFin bulletin 3.3.1	Review of the analysis of capital ratios
	<b>Risk Strategy</b>		
17 B	Does the risk strategy include an analysis of the impact of sustainability risks on risk universe/map/inventory?	BaFin bulletin 3.3.2	Review of the risk strategy with regard to the risk universe
18 B	Has the company defined risk indicators to assess the extent and time horizon of sustainability risks, taking into account risk appetite and risk-bearing capacity?	BaFin bulletin 3.3.2  ECB Guide, Expectation 4.2	Review of risk strategies and organizational policies  Review Risk Appetite Framework, -statement
19 D	Do the risk strategies contain rules on the frequency with which sustainability risks are taken into account in the risk inventory?	BaFin bulletin 3.3.2	Review of risk strategies and organizational policies

20 B	Are comprehensible, appropriate regulations for the measurement and management of concentration risks related to sustainability risks provided in the relevant risk strategies?	BaFin bulletin 3.3.3 ECB Guide, Expectation 4.2	Review risk strategies and organizational policies of the company
21 B	Does the company periodically review its risk strategies for identifying, assessing, managing, monitoring, and reporting physical and transition risks?	BaFin bulletin 3.3.4 ECB Guide, Expectation 7.4	Review of risk strategies and organizational policies of the company  Review of risk drivers/concentration risks (countries, sectors, products)
22 B	How does the company ensure that processes for identifying, measuring, managing, and reporting sustainability risks are improved? (systematically or selectively)	BaFin bulletin 3.3.5 ECB Guide, Expectation 7.4	Review of the processes for identifying, measuring, managing, and reporting sustainability risks
<b>Corporate Communications</b>			
23 B	How is the management's defined approach to sustainability risks communicated? (within management, with employees, contractual partners, investors)	BaFin bulletin 3.4	Retracing of communication to addressees
24 D	Are internal and external publications and pronouncements by members of management consistent with the company's sustainability goals?	BaFin bulletin 4.4	Review of in-house announcements, publications, press releases
25 B	How has the company decided whether to communicate to stakeholders with significant sustainability risks how such risks can be mitigated or reduced in the future?	BaFin bulletin 3.2.2	Follow-up of decision (e.g., committee minutes) whether to enter into a dialogue with third parties
26 B	Have any criteria for excluding or specifically managing certain risk positions been communicated to customers, stakeholders, etc.?	BaFin bulletin 3.4	Follow-up of communication to addressees

## 2 Business organization

	<b>Audit field and audit guiding questions</b>	<b>Note</b>	<b>Possible audit procedures</b>
	<b>Organizational Policies and Processes</b>		
27 B	Are sustainability risks adequately addressed in the relevant organizational policies (risk management, credit, investment, product, other relevant policies) and/or do stand-alone ESG policies exist?	BaFin Leaflet 5.1  ECB Guide, Expectation 3, 3.2, 3.3, 4, 4.1, 7.1, 8.5, 13.1	Analysis of organizational policies  Review of approval procedures, esp. NPP/product catalog.
28 B	Are the responsibilities (division of tasks, competencies) with regard to sustainability risks in the process organization adequately defined in the organizational guidelines? Is there a transparent and documented decision-making process?	BaFin bulletin 5.3  ECB Guide, Expectation 3.1, 5, 5.1, 5.3, 5.4	Analysis of organizational charts  Recording of the decision-making processes
29 D	Does the initial review of transactions with contractual partners or investment objects also include the identification and analysis of sustainability risks and are these included in the decision-making processes?	BaFin bulletin 5.2, 5.6  ECB Guide, Expectation 7.4, 7.5, 8.1	Process recording customer acceptance
30 D	Does the back office monitor the front desk's assessment of sustainability risks and compliance with relevant sustainability-related limits or exclusion criteria? Are limits and exclusion criteria sufficiently and clearly defined?	BaFin bulletin 5.2, 5.7  ECB Guide, Expectation 8.1, 8.3, 8.4	Process recording  Review of limit system

<b>Resources</b>			
31 B	How does the bank ensure that sufficient and appropriate human and other resources are available to address the new challenges of dealing with sustainability risks?	BaFin bulletin 3.2.4	Review of human resources planning, particularly in the area of risk management, with regard to the impact of sustainability risks
32 B	Have estimates been made for additional staffing requirements, e.g., in risk management?	BaFin bulletin 3.2.4	Review of human resources planning, particularly in the area of risk management, with regard to the impact of sustainability risks
33 B	Do ESG risk training programs exist for employees?	BaFin bulletin 3.2.4	Insight into internal training programs
<b>Sustainability Unit</b>			
34 B	Has an independent sustainability unit (SD) been implemented and what tasks does the SD assume and what risks does it consider?	BaFin bulletin 5.5	Review of organizational charts  Review of committee overviews and rules of procedure  Process recording
35 B	Is the SD appropriately integrated into the relevant existing processes and are the interfaces to other functions adequately defined?	BaFin bulletin 5.5	Review of organizational charts  Review of committee overviews and rules of procedure  Process recording
<b>Special Functions MaRisk</b>			
36 B	Have measures been taken to strengthen the expertise of the special functions as defined by MaRisk or other units within the institution with regard to sustainability risks?	BaFin bulletin 5.4  ECB Guide, Expectation 5.2	Review planning of training

37 D	Does risk controlling take sustainability risks into account as part of its activities and is there adequate reporting of significant sustainability risks to management ?	BaFin bulletin 5.2, 5.8 ECB Guide, Expectation 6, 6.3	Process recording Review Risk Reporting
38 B	Does the compliance function also consider the legal requirements for the sustainability of companies in the financial sector as part of its activities?	BaFin bulletin 5.2, 5.9 ECB Guide, Expectation 5.5	Process recording Review database of supervisory requirements
<b>Emergency Management</b>			
39 D	Are the main sustainability risks adequately considered in emergency management? Are exit strategies and corresponding processes established?	BaFin bulletin 5.11 ECB Guide, Expectation 9, 9.1	Analysis of emergency concept and emergency management process Process recording
<b>Outsourcing Management</b>			
40 B	How are sustainability risks taken into account in the case of significant or critical outsourcing, especially in the case of important or special functions (control and core banking areas)?	BaFin bulletin 8.1 BaFin Survey on Sustainability Risks, 14.10.2021, p. 22 MaRisk AT 9 para. 4, 5 MaGo ch. 13.4 § 36 KAGB	Review of outsourcing strategy and policies or guidelines Review of risk analyses
41 D	To what extent are sustainability risks taken into account in all outsourcing activities?	BaFin Survey on Sustainability Risks, 14.10.2021, p. 23 para. 2	Review of the methodology and completeness of various registers

42 B	Are responsibilities for sustainability risks in processes for all outsourcing and purchasing processes for other external purchases sufficiently clear and appropriately detailed?	MaRisk AT 5 para. 3	Review of the specifications in outsourcing and purchasing management
43 B	Are there standard regulations to be agreed with service providers with regard to sustainability risks?	BaFin bulletin 8.1 MaRisk AT 9 para. 7	Review of the contract system and model contracts
44 D	Are the reporting obligations of service providers sufficiently regulated to meet external sustainability reporting requirements?	BaFin bulletin 8.1	Review of the reporting requirements in the outsourcing agreements
45 B	Are sustainability risks properly included in the risk analysis for identifying material or critical outsourcing and the risks associated with outsourcing?	BaFin bulletin 8.2 ECB Guide, Expectation 9.1	Review of the risk analyses in the outsourcing process
46 B	In the case of significant or critical outsourcing, do the outsourcing contracts (if applicable, model contracts) contain appropriate requirements for the service provider to identify, assess, manage, monitor, and report on sustainability risks?	BaFin bulletin 8.3	Review of contracting, model contracts, or outsourcing agreements on specifications for service providers to properly incorporate sustainability risks into the service providers' risk management.
47 B	Do the organizational guidelines for central outsourcing management or the outsourcing officer contain appropriate and adequate regulations on processes for dealing with sustainability risks?	BaFin bulletin 8.4	Review of the organizational guideline outsourcing management
<b>Group Matters</b>			
48 B	Are there consistent group-wide policies and procedures) in particular on strategies, responsibilities, and risk management with regard to sustainability risks? Are these regulations implemented throughout the Group? Who is in charge for compliance?	BaFin bulletin 9.1	Review of group policies

49 B	Is there a central unit (e.g., sustainability unit) for group-wide sustainability risk management? If so, what are its main tasks?	BaFin bulletin 9.2	Review of organizational charts and organizational guidelines
50 D	How are sustainability concentration risks taken into account in risk management at Group level?	BaFin bulletin 9.3	Evaluation of the group risk strategy and framework
51 B	How is it ensured that sustainability standards, when applied, are observed by all companies in the Group?	BaFin bulletin 9.4	Review of committee documents, group guidelines, sustainability reporting
52 D	Are sustainability risks taken into account in the risk-bearing capacity calculation at Group level (especially in the economic perspective)?	BaFin bulletin 9.4	Review Risk-bearing capacity calculation group level

### 3 Risk Management

	<b>Audit field and audit guiding questions</b>	<b>Note</b>	<b>Possible audit procedures</b>
	<b>Risk Management Process</b>		
53 B	Are the tasks, responsibilities, and timeframe (defined cycle) for identifying, assessing, managing, monitoring, and reporting sustainability risks clearly defined and approved by management?	BaFin bulletin 6.1.1	Review of the sustainability criteria  Review/verification of strategies, policies and procedures in terms of completeness, timeliness and consistency of definition, responsibilities.
54 B	Are the methods and procedures for assessing, managing, monitoring, and reporting sustainability risks reviewed at regular intervals (in the sense of an adequacy check)?  Does this include the quality of the underlying data?	BaFin bulletin 6.1.2	Review risk inventory, esp. for central vs. decentralized responsibilities



55 B	<p>Are (physical and transitory) sustainability risks along with their impact on the effects on the well-known risk types (counterparty default risks, market price risks, etc.) considered in written risk management regulations? How are ESG risks transferred to the main risk types? Are sustainability risks that have a significant impact on the asset, income, and liquidity situation integrated into the existing risk measurement procedures?</p>	BaFin bulletin 6.1.3, 2.7, 6.6.1	<p>Review of risk inventory in terms of timeliness and completeness</p> <p>Review of the procedures for identifying new sustainability risks or changes resulting from them for the risk management process</p> <p>Review of the reporting</p>
56 D	<p>Do suitable processes exist for the early identification of sustainability risks?</p> <p>Do procedures exist to avoid or reduce sustainability risks (e.g., avoidance of reputational damage)?</p>	BaFin bulletin 6.1.3	<p>Process recording</p> <p>Attention to interfaces with other audits, e.g. complaint management, but also lending business (loan defaults in connection with environmental disasters), treasury (price changes), deposit business (customers' investment wishes)</p>
57 B	<p>Are escalation processes defined for involving the management level in dealing with sustainability risks?</p> <p>Are existing escalation processes used or supplemented to involve the management level in dealing with sustainability risks?</p>	BaFin bulletin 6.1.4	<p>Process recording</p> <p>Examination of escalation procedures (ad-hoc procedures as well as regular procedures)</p> <p>Review of the reporting</p> <p>Processes for handling complaints/incidents related to sustainability</p>

58 D	<p>Are appropriate risk indicators defined to assess the extent and time horizon for sustainability risks in the risk-bearing capacity and risk appetite?</p> <p>Can sustainability risks that are recorded under strategic, operational, or reputational risks also be quantified, in other words, what is the procedure for qualitative assessment?</p>	BaFin bulletin 6.1.5	<p>Reconciliation of strategies, risk inventory and their results with current KPIs</p> <p>Fit of KPIs with business areas/risks</p> <p>Evaluation of complaints/incidents</p>
59 D	Are sustainability risks taken into account in loan processing (loan granting and loan follow-up)?	BaFin bulletin 6.6.3	<p>Process recording Credit processes</p> <p>Note: Corresponding issues also arise for deposit business (customers), own investments/investment book</p>
60 D	Does the credit check identify and assess future risks, such as sustainability risks, in a complete, risk-oriented and appropriate manner (taking scenarios into account, if necessary) and, if applicable, verify them through independent sources?	BaFin bulletin 6.6.3	Process recording credit processes
61 D	Are internal bank findings and information taken into account in external credit checks?	BaFin bulletin 6.6.3	Process recording credit processes
62 D	Are sustainability risks (e.g., energy efficiency of real estate, flood events) also taken into account in the context of collateral valuations?	BaFin bulletin 6.6.4	Process recording credit processes , here: collateral processes

63 D	<p>Are internal and also external sources used to identify sustainability risks?</p> <p>Is data required for the risk management of sustainability risks held in accordance with BCBS 239?</p>	BaFin Fact Sheet 4.3	<p>Review of data flow diagrams</p> <p>Alignment with data governance and data quality guidelines</p> <p>Verification of certification from external sources</p> <p>Review of service level agreements</p>
64 B	<p>Are sustainability risks adequately addressed in internal reporting?</p> <p>Are quantitative vs. qualitative impacts sufficiently acknowledged?</p>	BaFin bulletin 6.5	Review risk reporting
65 D	<p>Are the special characteristics of sustainability risks (time horizon, interaction with other risks) adequately taken into account in the reporting? Qualitative or descriptive statements based on scenario analyses can also be formulated for this purpose.</p>	BaFin bulletin 6.5, 7.6	<p>Review risk reporting</p> <p>Comparison with scenario analyses</p>
<b>Risk Management Methodology</b>			
66 B	<p>Are there methods for managing and/or limiting sustainability risks that are consistent with the business and risk strategy?</p>	BaFin bulletin 6.2	<p>Alignment of control methods with business and risk strategy</p> <p>Review of risk inventory</p>
67 B	<p>Are exclusion criteria/limits defined for this purpose? For example, are certain customer transactions or sectors not carried out or only carried out to a limited extent?</p>	BaFin bulletin 6.2	<p>Alignment of control methods with business and risk strategy</p> <p>Review of risk inventory</p> <p>Keyword: clear and transparent communication regarding business activities</p>

68 D	<p>Alternatively, are appropriate positive lists drawn up (focus on specific companies, sectors, etc.)? Alternatively, are the companies in an industry selected that best meet the sustainability criteria (best-in-class approach)?</p> <p>Is the use of positive lists appropriately differentiated in order to avoid greenwashing, among other things?</p>	BaFin bulletin 6.2.2, 6.2.3	<p>Review of the positive lists</p> <p>Reconciliation with revenue strategy, as use may have an impact on the revenue situation because it is not flexible enough</p> <p>Review of the validation of positive lists (e.g., when using indices)</p> <p>Critical appraisal of the appropriateness of the procedure (if necessary, negative approach more suitable)</p>
69 D	<p>Was the determination of the above limits/positive lists also based on internationally recognized standards?</p>	BaFin bulletin 6.2.4	<p>Comparison of the definition procedures with relevant standards (e.g., UN-Goals, EU-Taxonomy)</p>
70 B	<p>Are risk analysis or classification procedures used to identify and assess sustainability risks, and is integration properly implemented?</p>	BaFin bulletin 6.3.1	<p>Review of procedural documentation</p> <p>Review of process changes (e.g., change requests)</p> <p>Review of system audits</p> <p>Review NPP process</p>
71 B	<p>Is the risk analysis or a risk classification procedure used to comply with legal and internal company requirements (e.g., limits/exclusion criteria)?</p>	BaFin bulletin 6.3.1	<p>Comparison with limit systems, exclusion criteria</p> <p>Review of the business strategy</p> <p>Inspection of controlling data (scope of business)</p>

72 B	Are risk mitigation or risk avoidance measures defined depending on the risk assessment of the contractual partner/investment object?	BaFin bulletin 6.3.1	Reconciliation with customer classification procedures/investment approval documentation.  Audit credit/collateral processes
73 D	Are business contract partners examined with regard to their affiliation with an emissions-intensive industry (incl. upstream and downstream supply chains)? An individual examination of the risk position should be carried out (external suppliers on the basis of a heat map are only indications).	BaFin bulletin 6.3.2	Review customer onboarding checklist  Sample customer file  Alignment with outsourcing process and operational functional areas
74 D	For higher risk transactions (e.g., indications of heat map sustainability risk), are more intensive analyses of the business model performed (e.g., to determine transition risk)?	BaFin bulletin 6.3.3	Review customer onboarding checklist  Sample customer file
75 D	Are appropriate measures to reduce the contractor's sustainability risk agreed and implemented?  How are these measures defined (action plan incl. schedule and reporting requirements)?  Is there reasonable tracking within the bank?  How are appropriate escalation processes defined in the event of non-compliance?	BaFin bulletin 6.3.4.3, 6.3.4.4	Process recording  Sample customer file
76 D	Are sustainability risks adequately taken into account in the design of the terms and conditions?	BaFin bulletin 6.3.5	Review contract conditions

77 B	<p>Are sustainability risk limits used to make transaction decisions?</p> <p>Do limit overruns lead to the rejection of transactions or is an escalation process initiated?</p>	BaFin bulletin 6.3.4.6	<p>Review of external appraisals, due diligence, credit decision submissions.</p> <p>Audit own investments/treasury</p>
78 B	Are sustainability risks considered completely, institution-specifically, and appropriately in the risk inventory or portfolio analysis?	BaFin bulletin 6.4	Review of risk inventory, portfolio analysis
79 B	Is the risk-bearing capacity also given in consideration of sustainability risks (incl. risk concentrations)?	BaFin bulletin 6.6.2	<p>Review of risk-bearing capacity calculation, risk inventory</p> <p>Review of committee decisions</p>
<b>Stress Test/Scenario Analyses</b>			
80 B	Do existing bank-specific stress tests adequately reflect sustainability risks? Are these taken into account in the stress testing framework?	BaFin bulletin 7.1	<p>Review stress testing framework</p> <p>Review scenario documentation</p>

81 D	<p>Are scenarios used that adequately and fully take into account physical as well as transitory risks and allow a statement on the resilience of the institution?</p> <p>Do the stress tests take into account scenario analyses that are plausible and sufficiently long-term? Are these regularly scrutinized and adjusted?</p>	BaFin bulletin 7.2	<p>Review scenario documentation with a focus on transitory risks (e.g., how will the promotion of electric cars be assessed in 10 years? What will the impact be 10 years from now due to what is perceived to be an environmentally friendly design today?)</p> <p>Plausibility check of the time horizon of the scenarios against the background of transitory risks</p> <p>Plausibility check of the scenarios with regard to physical risks</p> <p>Plausibility check regarding adverse scenarios</p>
82 D	When using Integrated Assessment Modeling (IAM) for transition scenarios, are scenario analysis methods critically appreciated?	BaFin bulletin 7.3	Review of specialist concepts evaluation models
83 D	Are realistic impact scenarios for physical risks created and modelled, covering a long-term time horizon?	BaFin bulletin 7.4	Review scenario documentation
84 D	Are several alternative scenarios, based on different combinations of assumptions, considered? Do these fit the bank's business model and risk profile?	BaFin bulletin 7.5	Review scenario documentation

<b>ESG Rating</b>			
85 D	Are ESG factors only taken into account in the credit rating if they have an influence on the creditworthiness of a company or the credit risk of a financial instrument?	BaFin bulletin 10.1 ECB Guideline para. 6.2 EBA GL LOM para. 126, 146	Process recording credit rating (process mining)
86 D	Are the ESG ratings used clearly distinguishable from the credit ratings used?	BaFin bulletin 10.2 ECB Guideline para. 6.2 EBA GL LOM para. 126, 146	Process recording credit rating (target/actual comparison)
87 D	Are there uniform standards for the ESG ratings used or do they comply with the EU taxonomy?	BaFin bulletin 10.3 ECB Guide para. 6.2 EBA GL LOM para. 126, 146	Comparison of ESG rating concept with, e.g., EU taxonomy  Critical appraisal of ESG data providers (certifications, etc.)
88 D	Have ESG ratings used been sufficiently validated with regard to the sustainability of a financial investment and have aspects of sustainability been distinguished from those of creditworthiness or credit risk as part of the validation process if these are unrelated?	BaFin bulletin 10.4 ECB Guide para. 6.2 EBA GL LOM para. 126, 146	Sample credit



## 4 Attachments

### 4.1 Feedback questionnaire

Thank you very much! DIIR would like to thank you for taking the time to evaluate the DIIR ESG Audit Guide and thereby contributing to the improvement of the guide by sharing your opinion! We look forward to your user experiences and opinions!

You can easily copy the following feedback questions into an email to [arbeitskreise@diir.de](mailto:arbeitskreise@diir.de) and send us your answers:

1. Overall, how helpful did you find the audit guide for your (a) initial audit or (b) follow-up audit?
2. Was the initial effort for an ESG audit lower with the use of the DIIR ESG Audit Guide than without its use?
3. How would you rate the complexity of the exam or the level of difficulty?
4. How did you find the handling of the audit guide and its structure?
5. How do you assess the applicability/relevance for your company?
6. Were the sources or further information possibilities apparent to you?
7. In your opinion, are there any questions or issues that are (a) not sufficiently presented/checked or (b) missing?
8. Is there anything else you would like to tell us or bring to our attention?
9. Was the "B" or "D" indicator helpful in your assessment of the audit fields, did you omit it from your audit, or are there any comments you would like to make about it?

## 4.2 Legal sources

German Federal Financial Supervisory Authority (BaFin): Merkblatt zum Umgang mit Nachhaltigkeitsrisiken, 1.10.2021, [https://www.bafin.de/SharedDocs/Downloads/DE/Merkblatt/dl\\_mb\\_Nachhaltigkeitsrisiken.pdf?\\_\\_blob=publicationFile&v=9](https://www.bafin.de/SharedDocs/Downloads/DE/Merkblatt/dl_mb_Nachhaltigkeitsrisiken.pdf?__blob=publicationFile&v=9) (as of 7.4.2022).

German Federal Financial Supervisory Authority (BaFin): Circular 10/2021 (BA) - Minimum Requirements for Risk Management (MaRisk), August 16, 2021, [https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2021/rs\\_1021\\_MaRisk\\_BA.html](https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2021/rs_1021_MaRisk_BA.html) (as of April 7, 2022).

German Federal Financial Supervisory Authority (BaFin): Sachstandserhebung Nachhaltigkeitsrisiken, 14.10.2021, [https://www.bafin.de/SharedDocs/Downloads/DE/Aufsichtsrecht/dl\\_Bericht\\_Umfrage\\_Sustainable\\_Finance.html](https://www.bafin.de/SharedDocs/Downloads/DE/Aufsichtsrecht/dl_Bericht_Umfrage_Sustainable_Finance.html) (as of 7.4.2022).

European Central Bank (ECB): Guidance on Climate and Environmental Risks, November 2020, <https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.202011finalguideonclimate-relatedandenvironmentalrisks~58213f6564.en.pdf> (as of 7.4.2022).

European Banking Authority (EBA): Guidelines on Lending and Supervision, EBA/GL/2020/06, May 29, 2020, [https://www.eba.europa.eu/sites/default/documents/files/document\\_library/Publications/Guidelines/2020/Guidelines%20on%20loan%20origination%20and%20monitoring/Translations/886677/Final%20Report%20on%20GL%20on%20loan%20origination%20and%20monitoring\\_COR\\_DE.pdf](https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/Guidelines%20on%20loan%20origination%20and%20monitoring/Translations/886677/Final%20Report%20on%20GL%20on%20loan%20origination%20and%20monitoring_COR_DE.pdf) (as of April 7, 2022).

Financial Stability Board (FSB): Recommendations of the Task Force on Climate-related Financial Disclosures, June 2017, <https://assets.bbhub.io/company/sites/60/2021/10/FINAL-2017-TCFD-Report.pdf> (as of 7.4.2022).

National CSR Forum of the German Federal Government: Berlin CSR Consensus on Corporate Responsibility in Supply and Value Chains, June 25, 2018, <https://www.bmas.de/SharedDocs/Downloads/DE/Arbeitsrecht/csr-konsens-lieferwertschoepfungsketten.html> (as of April 7, 2022).

German Council for Sustainable Development (RNE): The German Sustainability Code (DNK), <https://www.deutscher-nachhaltigkeitskodex.de/> (as of 7.4.2022).

UN Environment Program: Principles for Responsible Banking, <https://www.unepfi.org/banking/bankingprinciples/> (as of 7.4.2022).

UN Environment Program: Principles for Responsible Investment, <https://www.unpri.org/about-us/about-the-pri> (as of 7.4.2022).

UN Environment Program: Principles for Sustainable Insurance, <https://www.unepfi.org/psi/> (as of 7.4.2022).

### 4.3 Definitions

ESG	Environmental Social Governance (Environment, Social and Corporate Governance)
United Nations Sustainable Development Goals	17 United Nations Sustainable Development Goals (SDGs) <sup>1</sup>
Sustainability risks	<p>Sustainability risks within the meaning of the factsheet are events or conditions from the ESG (environmental, social or corporate governance) areas, the occurrence of which may actually or potentially have a significant negative impact on the net assets, financial position, and results of operations as well as on the reputation of a company; this includes climate-related risks in the form of <i>physical risks</i> and <i>transition risks</i>.<sup>2</sup></p> <p>BaFin sees sustainability risks as a partial aspect of the known risk types<sup>3</sup> - see MaRisk:<sup>4</sup> Credit risk/counterparty risk see <i>BTO 1 Lending business' BTR 1 Counterparty risks</i>, Market price risk see <i>BTR 2 Market price risks</i>, Liquidity risk see <i>BTR 3 Liquidity risks</i>, Operational risk see <i>BTR 4 Operational risks</i></p>
Physical risks	Physical risks results from both individual extreme weather events and their consequences (examples: Heat and drought periods, flooding, storms, hail, forest fires, avalanches) as well as long-term changes in climatic and ecological conditions (examples: Precipitation frequency and amounts, weather instability, sea level rise, changes in ocean and air currents, ocean acidification, increases in average temperatures with regional extremes).

---

<sup>1</sup> <https://unric.org/de/17ziele/>.

<sup>2</sup> BaFin: Leaflet on dealing with sustainability risks (consultation version 20.09.2019), p.14.

<sup>3</sup> BaFin: Leaflet on dealing with sustainability risks (consultation version 20.09.2019), p.14.

<sup>4</sup> BaFin: Circular 10/2021 (BA), Minimum Requirements for Risk Management (MaRisk).

Physical risks can also have indirect consequences (examples: Collapse of supply chains, abandonment of water-intensive business activities to climate-induced migration and armed conflicts).<sup>5</sup>

Transition risks	Transition risks exist in connection with the transition to a low-carbon economy: Political measures can lead to an increase in the price and/or shortage of fossil fuels (examples: coal phase-out, CO <sub>2</sub> tax) or to high investment costs due to the necessary renovation of buildings and plants. New technologies can displace familiar ones (example: electromobility), and changing customer preferences and societal expectations can endanger companies that have not adapted. <sup>6</sup>
Interdependencies	There are interdependencies between physical risks and transition risks. A sharp increase in physical risks would require a more abrupt change in the economy, which in turn leads to higher transition risks. <sup>7</sup>
Risk concentrations	In addition to risk positions ( <i>see sustainability risks</i> ) vis-à-vis individual counterparties that represent a risk concentration due to their size alone, risk concentrations can arise both from the synchronization of risk positions within a risk type (intra-risk concentrations) and from the synchronization of risk positions across different risk types (due to common risk factors or due to interactions of different risk factors of different risk types, inter-risk concentrations). <sup>8</sup>
Greenwashing	Sale of supposedly sustainable financial products <sup>9</sup>
Sustainable (financial) products	E.g., green bonds, social bonds, green loans, sustainable investment assets

---

<sup>5</sup> BaFin: Leaflet on dealing with sustainability risks (consultation version 20.09.2019), p.11.

<sup>6</sup> BaFin: Leaflet on dealing with sustainability risks (consultation version 20.09.2019), p.11.

<sup>7</sup> BaFin: Leaflet on dealing with sustainability risks (consultation version 20.09.2019), p.10.

<sup>8</sup> BaFin: Minimum Requirements for Risk Management (MaRisk), Explanatory Notes on Circular 10/2021 (BA) (August 16, 2021).

<sup>9</sup> BaFin: Leaflet on dealing with sustainability risks (consultation version 20.09.2019), p.14.

## Authors

This guideline was developed by the banking working groups of DIIR – Deutsches Institut für Interne Revision e.V.

<b>Name</b>	<b>Institute</b>
Matthias Frank Baumann	KfW
Stephan Bellarz	DZ BANK
Sebastian Franke	Deutsche Apotheker- und Ärztebank
Sebastian Huth	Landesbank Hesse-Thuringia
Tim Hustermeier	UBS Europe
Alexandra Kaltenbach	DekaBank
Alegra Konitzer	Berlin Savings Bank
Chris Mudrack	DKB Deutsche Kreditbank
Anna Reich (Management)	Helaba Landesbank Hessen-Thüringen
Carsten Rilinger	LBBW Landesbank Baden-Württemberg
Jens Roehr	Commerzbank
Mechthilde Roesch	B. Metzler seel. Son & Co.
Jill Round	KfW
Dominik Schäfer	German Bank
Sebastian Schaub	Taunus Savings Bank
Carsten Wulle	Helaba Landesbank Hessen-Thüringen

Published April 14<sup>th</sup>, 2022 at [www.diiir.de](http://www.diiir.de).

Translation into English published December 9<sup>th</sup>, 2022.

DIIR – Deutsches Institut für Interne Revision e.V. (IIA Germany)

Theodor-Heuss-Allee 108

60486 Frankfurt am Main