Shared Assessments
EBA Consultation Paper 2024-02 Regulatory Response

Date: April 16, 2024

To: European Banking Authority

Submitted Through: Online Portal

From: Andrew Moyad, CEO, Shared Assessments LLC

Subject: EBA/CP/2024/02 Consultation Paper: Draft Guidelines on the management of ESG risks

The Shared Assessments Program appreciates the opportunity to submit comments to the European Banking Authority Consultation Paper EBA/CP/2024/02 Draft Guidelines on the management of ESG risks.

Since 2005, Shared Assessments has been setting the standard in third party risk assessments. Shared Assessments, which is the trusted source in third party risk assurance, is a member-driven, industry-standard body that defines best practices, develops tools, and conducts pace-setting research. Program members work together to build and disseminate best practices and develop related resources that give all third party risk management stakeholders a faster, more rigorous, more efficient, and less costly means of conducting security, privacy, and business resiliency control assessments. Additional information on Shared Assessments is available by visiting: http://www.sharedassessments.org.

On behalf of the Program and its members, thank you for accepting the following response in regard to EBA/CP/2024/02 Consultation Paper: Draft Guidelines on the management of ESG risks.

Question	Response and Rationale
Question 1: Do you have comments on the EBA's understanding of the plans required by Article 76(2) of the CRD, including the definition provided in paragraph 17 [of the current Consultation Paper 2024/02] and the articulation of these plans with other EU requirements in particular under CSRD and the draft CSDDD?	**Response:** Shared Assessments Program comments are limited to the areas of the draft in which we have substantive responses on the proposed regulation as it pertains to critical supply chain risk management. We have indicated "No Response" for those questions that are outside of this area of focus. The meaning of the terms "counterparty," "portfolio," and "solvency" within the context of this proposal are not adequately defined. We recommend that the EBA more clearly and consistently define these terms to define more precisely the scope covered under these guidelines. The final guidelines should indicate how organizational mandates should be harmonized across multiple regulatory jurisdictions, when consideration of risks may have conflicting ESG-related risk management mandates. The draft adds a layer of impractical risk management guidelines because it includes "downstream activities" documentation that largely mimics existing guidelines under which financial institutions analyze their own footprint and ESG risk exposures. For example, CP 2024/02, Page 20, Section 24. "Institutions' internal procedures should provide for gathering information needed to assess the current and forward-looking ESG risk profile of counterparties, by aiming at collecting client and asset-level data." In this instance (Section 24), "large corporate counterparties" are "defined by Article 3(4) of Directive 2013/34/EU." Credit risk modeling might be applied to supply chain risk analysis; however, the feasibility of extending those models remains highly uncertain. Relative to the CSDDD, financial institutions will need only report on their internal and upstream activities (e.g., purchasing of equipment; not to the customers to how those institutions lend or the services the institution provides to its customers). Without clarifications of these specific questions, we have approached the content with our best understanding. **Rationale:** For example, the use of the term "counterparties" is stated on page 17 of this paper as "…used and defined in Directive 2013/36/EU and Regulation 575/2013/EU have the same meaning in these guidelines;" however, the term is used in ways that read as though the use expands beyond "central counterparties" from the regulation referenced definition. We recommend that the EBA narrow the scope of "counterparties" to define better what third and Nth party scope the EBA determines is minimally reasonable for regulated entities to "identify, measure, manage and monitor ESG risks, in particular environmental transition and physical risks, over long-time horizons, including through setting targets and milestones at regular time intervals." While the term counterparties is closely defined within these related laws, its use in many places within the draft to apparently include the vendor population. For example, not well-defined in those instances (e.g., Section 5.1, paragraph 43; page 18, paragraph 14c – additional examples as appropriate;). Therefore, we recommend that the EBA limit the use of "counterparties" and use another term (e.g., "vendor") to indicate providers. In addition, it is not clear about whether or how affiliates or vendors, such as utilities (Euroclear, ATM networks, ACH payments clearing, etc.) are included. The guidance should specify the type of "portfolios." For example, commonly referred to in regulatory guidance (market, credit, investment,…).

Question	Response and Rationale
	The term "solvency" is used in a variety of contexts, which could be interpreted to cover both solvency as an organization (having the ability to meet long-term financial obligations and continue operations long into the future) exclusively dedicated to the assets of a firm (loans, credit portfolio, etc.) and to risk to solvency through the potential failure of a critical vendor or loss that could result in loss of operational capacity. For example, Section 3.2, paragraph 9, reads: "These guidelines aim at enhancing the identification, measurement, management and monitoring of ESG risks by institutions and at supporting their safety and soundness as they are confronted with the short, medium and long-term impact of ESG factors. The guidelines contain requirements as to the internal processes and ESG risks management arrangements that institutions should have in place, including specific plans to address the risks arising from the transition and process of adjustment to relevant sustainability legal and regulatory objectives." Data gathering and responding to jurisdictional requirements are not well-defined. For example, subsection 24.i under Environmental Risks includes: "geographical location of key assets and exposure to environmental hazards (e.g. floods, water stress, soil erosion) at the level of granularity needed for appropriate physical risk analysis,…" Please clarify what de minimis "level of granularity" would be deemed appropriate for an institution to comply with the rule. Note, in Section 4.2.19, "the necessary data and information" is referenced. Section 3.4.2 notes that some institutions (SNCIs) may use less granular methodologies "…provided that this does not put at risk their ability to manage ESG risks in a sufficiently safe and prudent manner and in line with their materiality assessment." This could be interpreted in a manner that the institutions might be excluded from the mandate to perform sufficiently in depth due diligence to determine on an ongoing basis the materiality of ESG risks. Section 4.1.17 does note: 17. "By way of derogation from paragraph 16, institutions may consider some of the sectoral exposures referred to in paragraph 16 as not materially subject to environmental risks provided they are able to justify it, such as when those sectoral exposures show a high level of alignment with Regulation 2020/852 (EU taxonomy)."
Question 2: Do you have comments on the proportionality approach taken by the EBA for these guidelines?	**No Response.**
Question 3: Do you have comments on the approach taken by the EBA regarding the consideration of, respectively, climate, environmental, and social and governance risks? Based on your experience, do you see a need for further guidance on how to handle interactions between various types of risks (e.g., climate versus biodiversity, or E versus S and/or G) from a risk management perspective? If yes, please elaborate and provide suggestions.	**Response:** The EBA's focus on ESG risks is heavily skewed on environmental risks. While Section 3.5.26 notes in closing that "On the environmental and social materiality side, the economic and financial activities of counterparties or invested assets can have a negative impact on environmental and social factors, which could in turn translate into financial impact on the institution," human rights and community-level impacts are less respected for their short- and long-term potential impacts on an institution (reputational risk, sanctions risk, etc.). We recommend that the EBA pursue a stronger focus on the materiality of third party related social, civil, and political rights risks (e.g., jurisdiction, geopolitical, and location risk criteria, such as reported systemic violation of human rights in vendor populations). **Rationale:** While conceptually, the draft Guidance is environmentally-focused, we interpret the discussion around third-party related ESG risks as intended to guide institutions to assess and treat all ESG-related risks as applicable

Question	Response and Rationale
	pillars in different terms of proportionality, relevancy, and materiality. There is insufficient data availability for in-depth understanding of vendor populations, setting an unrealistic expectation at the most basic level for this guideline.
Question 4: Do you have comments on the materiality assessment to be performed by institutions?	**No Response.**
Question 5: Do you agree with the specification of a minimum set of exposures to be considered as materially exposed to environmental transition risk as per paragraphs 16 and 17, and with the reference to the EU taxonomy as a proxy for supporting justification of non-materiality? Do you think the guidelines should provide similar requirements for the materiality assessment of physical risks, social risks and governance risks? If yes, please elaborate and provide suggestions.	**Response:** We agree that a minimum set of supply chain risk exposures considered material for environmental transition should be taken into account (as per paragraphs 16 and 17 of the Consultation Paper) to support justification of non-materiality where applicable – at minimum – as listed below in Annex I to Regulation (EC) No 1893/2006 Section L Real Estate Activities and Sections A-H: Agriculture, Forestry & Fishing; Mining & Quarrying; Manufacturing; Electricity, Gas, Steam & Air Conditioning Supply; Water Supply, Sewerage, Waste Management & Remediation Activities; Construction; Wholesale & Retail Trade – Repair of Motor Vehicles & Motorcycles; Transportation & Storage. We recommend that the guidelines provide for similar requirements for assessing materiality of physical, social, and governance risks for third parties outside this limited list (Annex I to Regulation (EC) No 1893/2006 Section L and Sections A-H). Financial institutions are exposed to significant risk by parties in other sectors. Examples of additional key exposure points through third and Nth parties are included in Annex I to Regulation (EC) No 1893/2006 Sections A-U Inclusive. Data processing, including data centers, under Annex I, Section J Information and Communication, 63.1 should be included in criteria, due to the high energy use and community-level impacts (e.g., noise, job siphoning) that are reported in communities where large centers have or are being established. The final rule should take into consideration the challenges associated with onsite assessment capabilities within this and other service sectors. **Rationale:** The increasingly fragile environment across sectors and supply chains dictates that institutions understand and assess the materiality of operational risk factors that extend beyond the minimum setoff exposures identified in the draft. Risk assessment must include geopolitical risks, including but not limited to: hyperactivity of state and non-state gang activity; location-specific climate risks that are compounding factors for geopolitical risks; climate-related (wildfires, hurricanes, shifting climate impacts across regions) changes to the frequency and severity of climate events; and economic fragility that results from these two risk areas. Risk assessment in the supply chain now requires institutions to determine what levers can be used to decrease risk (e.g., use of decentralized infrastructure by key provider that support power supply for operations, such as data centers and server farms, where disruption to centralized power sources would otherwise disrupt the stability or availability of outsourcer or sector activities).
Question 6: Do you have comments on the data processes that institutions should have in place with regard to ESG risks?	**Response:** We recommend that the EBA require data reporting based on Corporate Sustainability Reporting Directive (CSRD) requirements.

Question	Response and Rationale
	Rationale: While the need to collect pertinent data and conduct relevant analyses exists now, the ability to do so is not currently available. The data sources necessary to gauge vendor population activities and impacts may not exist, perhaps outside of environmental impacts. The EBA notes in Sections 4.2.1.24 and Section 3.1.4 (page 5) that while the need for accurate and appropriate data exists now; "However, the specificities of ESG risks such as their forward-looking nature and distinctive impacts over various time horizons as well as the lack of relevant historical experience means that understandings, measurements and management practices can differ significantly across institutions."
Question 7: Do you have comments on the measurement and assessment principles?	**Response:** The assessment measures are sound. We recommend that the EBA pursue a stronger focus on quantifying the materiality of third party related social, civil, and political rights risks (e.g., jurisdiction, geopolitical, and location risk criteria, such as systemic violation of human rights in vendor populations). The CSDDD would require that the institution correct material ESG risks, rather than manage those risks. Note that in Section 4.2.2, paragraph 27c, requires "Institutions' internal procedures should include tools, methodologies and capabilities to: a) identify ESG risk drivers and their transmission channels to prudential risk types and financial risk metrics via the institution's exposures; b) map exposures and/or portfolios according to ESG risk drivers, and any concentration within or between them, c) measure and manage material ESG risks including with a forward-looking perspective." **Rationale:** Metrics that are not quantifiable render analysis less plausible and decision-making less reliable. These ESG-related third and Nth party risks can be quantified by institutions as part of their ongoing risk assessment and horizon scanning processes through use of Open FAIR or similar models.
Question 8: Do you have comments on the exposure-based methodology?	**Response:** Establishing metrics for transition risks and for first steps for sector-level characteristics throughout the supply chain will help institutions establish benchmarks internally as well as against peer institutions. The issues posed around obtaining useful vendor data would make it necessary for the EBA to clarify and possibly narrow its definition of counterparty to allow for institutions to be able to fulfill the requirements of this section (e.g., Section 4.2.3, paragraph 32). **Rationale:** For metrics on social governance factors, as noted in Section 4.2.2. paragraph 29, quantifiable jurisdictional metrics related to environment, rights, equality, and resource use could be useful to add to guidelines for institutions. Section 4.2.3, paragraph 32." Where data needed to assess certain criteria is not yet available, such as for smaller corporate counterparties, institutions should first seek to engage with clients to obtain the data or consider using sector-level characteristics as a first step and, when feasible, operate adjustments to account for counterparty-specific aspects." Executing this is not feasible. For example, it would require gaining sector-level characteristics for AWS server farms for EU-based institutions that are supported by a US-based organization. This is just one example of a vendor that may be a material supplier in fact, even in the face of regulators routinely ruling out electric grid and cloud providers as critical suppliers.

Question	Response and Rationale
Question 9: Do you have comments on the portfolio alignment methodologies, including the reference to the IEA net zero scenario? Should the guidelines provide further details on the specific scenarios and/or climate portfolio alignment methodologies that institutions should use? If yes, please elaborate and provide suggestions.	**No Response.**
Question 10: Do you have comments on the ESG risks management principles?	**Response:** Within these principles, as defined, the 10- to 30-year horizon may be inadequate for risk management purposes in this industry. The management principles that require engagement with "counterparties" is sound. However, we recommend that the EBA use a risk-based management process, which, for example in Section 5.8, paragraph 72, mandates metrics such as using a percentage or a ratio that is not risk-based. **Rationale:** Scenario development and horizon scanning that is beyond a 30-year timeframe, while desirable, will have low confidence; however, events that fit within that 30+ year timeframe can also have very high impacts that need measurement without adequate data to accomplish this task. Currently, climate modeling for credit risk exposure does not apply to third parties. Those models might be applied across the supply chain to evaluate risks more completely.
Question 11: Do you have comments on section 5.2 – consideration of ESG risks in strategies and business models?	**Response:** The strategy and business models described are basic to building a comprehensive understanding of an institution's ESG-related risk exposures. Financial institutions, as part of daily activities, are using models that examine the risks being discussed. However, as high level stratagem and models, they are not practical for evaluating ESG risk exposures across the complete financial sector supply chain ecosystem. Having regulator-defined scenarios would ease the burden of individual institutions developing their own bespoke processes. Such an approach could be adapted by the regulator over time as a more stable business environment emerges. Until that time, the management of transition risk must be a priority, along with the unknowns contained in scenario analyses (present, short-term, long-term). **Rationale:** The 10- to 30-year horizon may be inadequate for climate and environment stress-testing. To be effective in meeting the EBA's overarching goals, institutions should exercise a willingness to explore models and strategies that have promise for the most robust and resilient investment, even if those models and strategies currently fall outside common practice. This consideration speaks to the need for environmental scenario analyses taking into account the context of environment and changes to economic drivers where climate-related impacts above 2C already need consideration in a business and political environment where 1.5C is already an obsolete goal. The goal of reducing firms impacts on not only the environment but also the social fabric has to be an achievable goal with the stated strategy. Providing an EU standard for what is sustainable (e.g., use of resources in a sustainable way that protects cultural and social needs – human rights, labor, governance – that are tied to environmental risks

Question	Response and Rationale
	in a given region), for instance, would defray the divergent strategic approaches that would arise due to institutions and companies seeking measurements that would allow operations to continue within their preferred (self-defined) thresholds, even where those thresholds do not provide sound social, governance, or environmental practices.
Question 12: Do you have comments on section 5.3 – consideration of ESG risks in risk appetite?	**Response:** The guidelines are sound. Institutions will have to determine the parts of their vendor ecosystem considered critical in ESG risk assessment to meet the provision that "…internal control framework should include a clear definition and assignment of ESG risks responsibilities and reporting lines." Focusing on solvency metrics as a solution to making this determination may result in two strategic camps: (1) making the vendor population as controllable as possible; and (2) making ESG a must-have, critical metric that all vendors must meet – neither of which is sustainable within financial markets. **Rationale:** The wide range of potential impacts from third and Nth parties, such as data center energy use and the potential for disruption of those centers, will have knock-on, revenue-related impacts that would need to be built into the real-world risk appetite (and related KPIs and KRIs) for far reaching impacts, such as those related to reputation risk that can arise from ESG-related risks. Without clarification on "counterparties," as written, the guidelines are unrealistic for institutions to include this cascaded risk in their risk appetite due to the lack of control that institutions have over cascading elements/components within their portfolios (credit/investment/etc.), including vendor portfolios.
Question 13: Do you have comments on section 5.4 – consideration of ESG risks in internal culture, capabilities and controls?	**Response:** The guidance in Section 5.4.23.b indicating the use of approval for new products with ESG features or significant changes to existing products to embed ESG features may be helpful in gaining an enterprise-wide acceptance of adopting behaviors into company culture that will advance product development along socially responsible lines. The draft calls for ESG to be included in ERM in Section 5.1, paragraph 41. While Section 5.4, paragraph 53.c, indicates practices that are commonly undertaken in larger entities, requirements are unclear to meet the examination by the compliance and risk management functions for all product features, though those examinations would be conducted on ESG risks related to new products or services. **Rationale:** To build an appropriate level of company culture and behavior, in which appropriate, repeatable processes are executed, requires an understanding of all aspects of a third party provider's supply chain, including products and platforms attached to an institution's networks and other operational systems. This is not achievable within the constraints posed by collecting data across the current supply chain ecosystem.
Question 14: Do you have comments on section 5.5 – consideration of ESG risks in ICAAP and ILAAP?	**Response:** While paragraph 59 presents the essential point that "institutions should take into account their size and complexity," an essential point worth adding is that their supplier ecosystem is important to consider within that complexity. **Rationale:** The supplier ecosystem in many instances will extend the ESG and operational risks of an institution's size and complexity, and ICAAP and ILAAP scenarios should incorporate these related risks as well.

Question	Response and Rationale
Question 15: Do you have comments on section 5.6 – consideration of ESG risks in credit risk policies and procedures?	**No Response.**
Question 16: Do you have comments on section 5.7 – consideration of ESG risks in policies and procedures for market, liquidity and funding, operational, reputational and concentration risks?	**Response:** Simulation, analysis, and reporting applied to other risk modeling could be extended to calculating and reporting the types of risks described in Section 5.7 of the Consultation Paper Guidelines. We recommend adding to Section 5.7, paragraph 63, "d) environment is the extended enterprise supply chain." (e.g., technology providers, cloud providers, etc. that may have extended ESG impacts). **Rationale:** While all necessary data will not be available to predict an outcome with absolute certainty, simulations can be used to gain insight into possible outcome(s) and the related probabilities of occurrence and potential impacts. These models can be utilized for individual vendors, all vendors, a type of vendor, or for evaluating internally-generated risks, including market, liquidity and funding, operational, and reputation risk. While risks at the institutional level may be assessed, institutions would remain unable to identify cascading risk from providers effectively where unknown concentration risk exists and/or cure for such risk where sole providers are present sector-wide.
Question 17: Do you have comments on section 5.8 – monitoring of ESG risks?	**Response:** In principle, the monitoring guidelines are sound. In practice, they will be difficult to execute and manage. Please also refer to the response to Question 10. **Rationale:** There will be supply chain risks that institutions would not be able to identify or monitor effectively in the institution's supply ecosystem.
Question 18: Do you have comments on the key principles set by the guidelines for plans in accordance with Article 76(2) of the CRD?	**Response:** The key principles set by the guidelines for plans in accordance with Article 76(2) of the CRD are sound; however, the guidelines in Section 6.1 of the Consultation Paper may be hindered from the lack of visibility into the supply chain. A key issue is that the guidelines relative to parent-subsidiary are not clear. Section 6.1, paragraphs 81-82, is clear if the parent company is located in the EU. However, what remains unclear are the requirements relating to counterparties (third parties) or if the subsidiary is headquartered in the EU, but the parent company is located outside the EU. It would be difficult for institutions to determine in this instance where the most stringent requirement lies to apply to their program. **Rationale:** Determining what are considered "adequate resources allocated to the management of all material risks addressed in this Directive and in Regulation (EU) No 575/2013 as well as in the valuation of assets, the use of external credit ratings and internal models relating to those risks" for this same reason. It is reasonable that "the institution shall establish reporting lines to the management body that cover all material risks and risk management policies and changes thereof."
Question 19: Do you have comments on section 6.2 – governance of plans required by the CRD?	**Response:** The governance of plans as required by the CRD are in harmony with Section 6.2 of the Consultation Paper Guidelines. The need to be ESG-aware and have consistent processes to raise that awareness is appropriate. However, Section 62, paragraph 86.a is not consistent with the commonly applied risk management principles in

Question	Response and Rationale
	which the role of being "responsible for establishing a dialogue with counterparties about their own transition plans and assess consistency with the institution's transition planning" is fulfilled by the second line of defense. **Rationale:** Not applicable.
Question 20: Do you have comments on the metrics and targets to be used by institutions as part of the plans required by the CRD? Do you have suggestions for other alternative or additional metrics?	**Response:** We recommend that the EBA require data reporting based on Corporate Sustainability Reporting Directive (CSRD) requirements. The metrics as described in this draft are heavily skewed to a few environmental factors to the exclusion of some key solvency metrics that would need to be met by vendors (counterparties). Without additional guidance on the definition of counterparty, as previously indicated, these measures are self-limiting. Additional metrics could include jurisdiction, geopolitical, and location risk criteria, such as the following: jurisdictional regulations to control and arbitrate the use of resources; civil, political, and other human rights and freedoms; and systemic violation of rights. **Rationale:** The use of metrics that tie more directly to Section 3.5, paragraph 25 of the Consultation Paper Guidelines would be valuable. "While institutions are more advanced on the measurement and assessment of climate-related risks, it is important that institutions progressively develop tools and practices that aim at assessing and managing the impact of a sufficiently comprehensive scope of environmental risks, extending beyond climate-related ones, such as risks stemming from degradation of ecosystems and biodiversity loss, as well as of other ESG factors." (Section 3.5, paragraph 25).
Question 21: Do you have comments on the climate and environmental scenarios and pathways that institutions should define and select as part of the plans required by the CRD?	**Response:** The confidence levels with which firms are going to be able to provide assurance will vary as a function of sustainability planning efforts within jurisdictional limits (i.e., the continuity of plans across jurisdictions).
Question 22: Do you have comments on section 6.5 – transition planning?	**Response:** The guidance in Section 6.5, paragraph 105 supports the overall precept that "Institutions should ensure that their transition planning and any planned shifts in financing activity will be accompanied by updated risk management policies such as procedures." Extending this assessment into supply chain risk management conceptually and practically to gauge vendor transition planning would be too broad a set of metrics to be practically assessed and monitored. **Rationale:** Conceptually, the guidance for transition planning is sound; however, the layer of risk management will be duplicative – in whole or in part – to existing guidance and would add an unnecessary burden unless the EBA defines the delta between existing rules and this new ESG guidance and is able to establish the value of that duplication.
Question 23: Do you think the guidelines have the right level of granularity for the plans required by the CRD? In particular, do you	**No Response.**

Question	Response and Rationale
think the guidelines should provide more detailed requirements?	
Question 24: Do you think the guidelines should provide a common format for the plans required by the CRD? What structure and tool, e.g., template, outline, or other, should be considered for such common format? What key aspects should be considered to ensure interoperability with other (e.g., CSRD) requirements?	**Response:** A common format would provide efficiencies for all parties (institutions/firms and regulators). An additional benefit of collecting information in a consistent manner would be that it can be more easily analyzed across institutions. Standardization should also reduce the cost of compliance and enable smaller institutions to compile the same type data as larger institutions, while allowing for "drill down" criteria not required of SNCIs. **Rationale:** A format that is common and leverages existing ESG-related analysis and reporting would provide benefits to institutions, regulators, as well as to vendors that would be contractually required to report specific data to their customers.
Question 25: Where applicable and if not covered in your previous answers, please describe the main challenges you identify for the implementation of these guidelines, and what changes or clarifications would help you to implement them.	**No Response.**
Question 26: Do you have other comments on the draft guidelines?	**No Response.**