Terms of Reference
Implementation of the Spain Enterprise Surveys, 2024

1. Background

The SPAIN ENTERPRISE SURVEYS 2024 (Spain ES 2024) is a World Bank (WB) establishment-level survey, whose objective is to gain an understanding of firms' day-to-day experiences and perceptions of the business environment in which they operate. The survey covers several topics including access to finance, corruption, infrastructure, competition, and performance measures. The survey methodology and questionnaire are standardized to reduce measurement error, ensure national representativeness, and to improve cross-country comparability. More information can be found at www.enterprisesurveys.org.

The Spain ES 2024 will also include re-visiting previously interviewed establishments, also known as "panel firms"; this allows for the creation of a panel dataset. The panel dataset allows researchers to track changes in the business environment over time and to assess the effects of business-enabling reforms initiated by the government. The WB will provide the selected Vendor (henceforth the "Vendor") with the names and contact details of the firms previously interviewed so that the Vendor is able to locate these firms, determine their eligibility status, and re-interview eligible panel firms.

2. Objectives

The Spain ES 2024 has the following objectives:

- Collect data from establishments on their day-to-day experiences;
- Produce robust business environment indicators that are comparable across countries;
- Produce measures of establishment-level performance, including productivity;
- Assess the constraints to private sector growth and establishment performance;
- Provide data that will be used for the World Bank's Business Ready project (B-READY);
- Build a panel dataset in applicable countries.

The overall goal of the Spain ES 2024 is to support evidence-based policy-oriented analysis, stimulate systematic policy dialogue on the business environment, and help shape the agenda for business-enabling reforms.

In addition to the core activity of the implementation of the Enterprise Survey(s), this project includes a supplementary task of providing the remuneration to experts involved in the World Bank's Business Ready project; this activity is described in further detail below (see section 3.6).

3. Scope of Work and Tasks

3.1 Survey Scope and Country Coverage

A total of 1,440 interviews are to be conducted by September 30, 2024 with the owner or top manager of each establishment. For larger establishments, select sections of the questionnaire can also be completed with specialized department managers that can provide more accurate responses for the corresponding topics (e.g., detailed breakdowns of employment, selected accounting figures, etc.). Due to the sensitivity and privacy of some of the information collected, in the past, data has been primarily collected via face-to face interviews; however, alternatives forms of data collection such as virtual interviews or a combination of modes of data collection could be considered, under the prior approval of the World Bank Task

Manager (TTL). The main criteria for the decision of alternative modes of data collection will be the maximization of response rates without compromising the representativeness of the achieved sample and without negatively affecting the quality of information. The survey will be conducted in Spain.

An indicative breakdown of the number of interviews by region, business sector, and size is provided in Table 1. This breakdown may be modified by the WB based on the sampling frame used for fieldwork.

Table 1 – Enterprise Survey (ES) stratification levels and overall targets

Region	Size	Food	Fabricated Metal Products	Machinery & Equipment	Furniture	Other Manufacturing	Retail	Other Services	TOTAL
Galicia	Small (5-19)								
Galicia	Medium (20-99)								
Galicia	Large (100+)								
Northwest	Small (5-19)								
Northwest	Medium (20-99)								
Northwest	Large (100+)								
Basque Community	Small (5-19)								
Basque Community	Medium (20-99)								
Basque Community	Large (100+)								
Northeast	Small (5-19)								
Northeast	Medium (20-99)								
Northeast	Large (100+)								
Community of Madrid	Small (5-19)								
Community of Madrid	Medium (20-99)								
Community of Madrid	Large (100+)								
Castile-Leon	Small (5-19)								
Castile-Leon	Medium (20-99)								
Castile-Leon	Large (100+)								
Center	Small (5-19)								
Center	Medium (20-99)								
Center	Large (100+)								
Catalonia	Small (5-19)								
Catalonia	Medium (20-99)								
Catalonia	Large (100+)								
East	Small (5-19)								
East	Medium (20-99)								
East	Large (100+)								
South	Small (5-19)								
South	Medium (20-99)								
South	Large (100+)								
Canary Islands	Small (5-19)								
Canary Islands	Medium (20-99)								
Canary Islands	Large (100+)								
	TOTAL								1,440

The breakdown follows the stratification criteria in the ES global sampling methodology. More information about the sampling methodology is provided in section 3.3 and in the Enterprise Surveys sampling note on the ES website.[1]

The primary objective of the survey project is to reach the target number of establishments for each business sector, region, and size group (stratification category) as described in these Terms of Reference (ToR). However, if the available sample of prospective respondents is exhausted before reaching the target number of interviews for a stratification category, the Vendor may be asked to use sample in other stratification categories to conduct additional interviews in order to reach the total number of interviews for each stratum. This procedure can only be used after consultation and authorization by the WB Task Manager (TTL).

Only formal (registered) establishments with five or more employees will be included (exceptions are made for panel firms that may have fewer than five employees). The standard Universe under study of the Enterprise Survey is the formal, private sector defined as all establishments with at least some percentage of private ownership in the sectors eligible for the study. Fully government-owned firms are excluded. The agricultural and extractive sectors are also excluded. In terms of the United Nations ISIC Revision 4.0, the Universe includes: manufacturing (group C), construction (group F), retail, wholesale and repair of motor vehicles (group G), transportation and storage (group H), accommodation and food services (group I), subsectors 58, 61, and 62 from information and communication (group J), professional, scientific, and technical activities (group M), subsector 79 from administrative and support services (group N) and subsector 95 from other service activities (group S).

3.2 Survey Instruments

3.2.1 The Questionnaire

The Enterprise Survey questionnaire, which includes several topics on the business environment, is designed to seek opinions and information from the establishment's senior manager, accountant, and/or human resource manager. These main sections are designed to be answered by the Top Manager or CEO. Two sections of the questionnaire may be better answered by the Human Resources Manager (employment or labor section) and the CFO or Accountant of the establishment (productivity section that is supposed to be taken from the establishment's financial statements). From experience, it is estimated that it may sometimes take two (2) visits/interviews to gather all data from medium to large manufacturing establishments. For the retail sector, small manufacturing establishments, and for establishments that are interviewed as part of the other services sample, the interviews can usually be completed in one visit. Experience shows that the full questionnaire may take approximately 60 minutes to implement.

The questionnaire is slightly different between manufacturing and services interviews. To save time, certain questions that may not be applicable to some establishments are eliminated (e.g. manufacturing-specific questions are not asked to retail and other services establishments.) The TTL will deliver the questionnaire to the Vendor. The questionnaire has already been developed; however, it will be finalized after the pilot interviews takes place to reflect country-specific variation in some of the survey concepts. It is intended that before beginning the piloting work, all parties, including the Vendor, should be confident that the surveys will achieve the objectives and can be completed within the budget provided for the surveys.

[1] http://www.enterprisesurveys.org/Methodology

In addition to the Questionnaire used to carry out interviews, the Vendor will use a Screener questionnaire (the "Screener") to 1) determine if establishments are eligible to be included in the survey and 2) make an interview appointment with eligible establishments. The Screener was designed to be implemented over the phone, but the Vendor must devise alternative strategies to complete it for cases where phone contact is not feasible. The Vendor is responsible for setting up any necessary computer-assisted telephone interview (CATI) to support screening and recruitment. This includes administering the Screener in person. Note that the World Bank has developed a Survey Solutions script for the Screener, and this can used by the Vendor.

During the screening process, establishments that refuse to participate or establishments which cannot be contacted (after multiple attempts), will be substituted with establishments having similar characteristics in the sample and following the preference order as provided by the TTL. Using the information collected from the Screener, only the TTL is authorized to set the rules for substitutions. All of the essential information collected with the Screener questionnaire is considered a deliverable of this survey project. In some countries, the Screener may have to be implemented via face-to-face for respondent businesses that lack phone contact information.

The Vendor will be expected to record the eligibility status of all the establishments that are contacted during the screening process, and to update contact information such as accurate addresses, emails and phone numbers. The TTL will provide a standard Excel file for this report. At the end of the project, the full report, for all firms contacted during the screening process, interviewed or not, will be a deliverable of the project using the Excel file provided by the TTL.

3.2.2 CAPI

It is expected that the survey data collection will use computer-assisted personal interviews (CAPI), which will comply with the basic checks, values, and skip patterns in the codebook provided by the TTL. To expedite implementation and to start fieldwork as soon as possible, the WB will provide the CAPI script for the questionnaire in "**Survey Solutions**", which will ensure consistency in data collection across all projects and accordance with the global codebook. The WB will provide the necessary servers to host Survey Solutions to facilitate data collection. The Vendor is responsible for coordinating with the WBG TTL any changes required in the script that arise from training, piloting, and/or fieldwork. More information about Survey Solutions is available here: http://support.mysurvey.solutions/. The Vendor should be prepared to coordinate field management and data collection using the built-in capabilities of Survey Solutions. The Vendor is also responsible for documenting any proposed updates to the questionnaire, including updates to questions, labels, variables, consistency patterns and/or checks that will have to be incorporated into the CAPI script. The final CAPI script must be approved by the TTL. All CAPI devices must have GPS capabilities.

Should any alternate or any combinations of modes of data collection be utilized, the Vendor is responsible for scripting, translation, and ensuring consistency of those scripts. Alternate modes of data collection require approval by the TTL.

3.3 Sampling Methodology

3.3.1 Sampling

The Spain ES 2024 will be stratified by business sector, size, and location within a country (for further details refer to Table 1 in section 3.1). The levels of stratification by business sector and location are determined by the size of each economy. The stratification by size will be distributed across three size categories based on the number of employees: small (5–19), medium (20–99), and large (100 or more). No establishments with fewer than five (5) employees will be surveyed, except for panel firms, as explained above.

The Vendor is responsible for obtaining the Universe table, that is the tabular counts of the total number of establishments in the country disaggregated by business sector, size, and location. The format of this table is provided in Appendix I.

The drawing of the sample, from the sampling frame, will be implemented by the WB TTL. The WB reserves the right to ask the selected Vendor to draw the sample following guidelines provided by the WB; if so, the contract will be revised accordingly.

3.3.2 Sampling Frame

Obtaining the sampling frame is a vital step prior to the beginning of fieldwork. To expedite the implementation of the project, the WB is taking steps to obtain the sampling frame for the project. The format table is provided in Appendix II. As indicated below, Vendors will only be responsible for testing the sampling frame provided, at the request of the WB TTL. Obtaining the sampling frame is not a deliverable, but after the contract has been signed and issued, the WB TTL may issue an amendment to the contract, if this deliverable needs to be added to the project scope and budget.

The attributes of an optimal sampling frame are:

- The sampling frame should include all operating establishments in the following sectors according to ISIC Rev. 4.0: all manufacturing (group C), construction (group F), retail, wholesale and repair of motor vehicles (group G), transportation and storage (group H), accommodation and food services (group I), subsectors 58, 61, and 62 from information and communication (group J), professional, scientific, and technical activities (group M), subsector 79 from administrative and support services (group N) and subsector 95 from other service activities (group S).

- In addition to completeness with respect to sector breakdown, the sampling frame should be the most updated list available in the country, containing information about the number of employees, and current address, phone number or other contact information for each establishment.

- At least one hundred (100) firms should be contacted to check the accuracy of the information of the sampling frame. The Vendor may also be required to perform desk research and complete the information necessary to locate potential firms. Names, contact information, business sector, size, and other relevant information may not be up to date or missing from the sampling frame; hence the Vendor may need to take necessary steps to complete the missing information.

- Ideally, the unit of the sampling frame should be the establishment, defined as a physical location or place of business, either production or services, with its own management decisions and cost/revenue accounting. If the best available frame is instead composed of firms (legal entity that may be composed of one or several establishments), this should be clearly stated. Special care should be taken when putting together frames from secondary sources to ensure their compatibility in terms of whether the original sources are establishments or firms.

3.4 Translation of Questionnaires and Other Survey Materials

A logistical step already undertaken by the World Bank is the translation of all survey materials. The Vendor is responsible for checking the translations provided by the WB TTL and providing corrections as necessary to ensure they are localized and clearly understood in each country. The survey interview documents include the questionnaire, questionnaire manual, Survey Solutions CAPI script, show cards, tip sheet, and invitation letter; these all are translated into the local language(s). The Vendor is also responsible for checking the translation of the CAPI material- both the text of the questionnaire and the internal messages and warnings for enumerators- into all local languages used for the survey fieldwork and

making any necessary changes to the translations accordingly. The Vendor is responsible for checking the translation of all training materials which include a few PowerPoint presentations, an exam for interviewers, and mock interview materials.

3.5 Survey Implementation

The Spain ES 2024 will be carried out by the selected Vendor by means of face-to-face interviews (or using alternatives modes of collection, as indicated above) with each establishment's top manager and potentially other senior managers as discussed above. Screening and post-interview follow-ups are usually implemented by phone. While the ES have been typically carried out by means of face-to-face interviews, recently, alternative modes of collection of information via videoconference are encouraged as a substitute to face-to-face interview whenever possible to increase the rate of response and increase the quality of the information. The use of alternative modes of collection will be discussed and authorized by the TTL. Face-to-face interviews are required when the technology for remote interview is not available or is considered sub-optimal.

Keeping limited personal data on individuals (name and contact information) may be needed by the Vendor for a limited period during fieldwork to conduct call-backs and implement quality controls. When collecting and processing personal data, the Contactor must fulfil its obligations as outlined in the Data Protection Annex (Annex 1). The Vendor must have encryption controls for information that will be stored (data at rest) and/or transmitted (data in motion/in transit) to the World Bank. The Vendor must apply rigorously, its policies and procedures, for the collection, safekeeping, processing, management and deletion of personal data, to ensure personal data collected by the Vendor remain confidential and are processed and managed in accordance with applicable law and best international standards throughout the time needed for fieldwork. Aside from contact information for the respondent establishment, the Vendor shall not communicate any personal data to the WB. The Vendor must destroy the collected personal data within a period of 12 months after the completion of the project. Moreover, the Vendor must remove any personal data from the tablets used for data collection after project completion.

3.5.1 Panel Data

Panel firms are defined as establishments from the previous Enterprise Survey wave. The ES place a high priority on re-interviewing panel firms in countries with available panel information.
Consequently, it is expected that the Vendor will have a clear strategy for contacting and recruiting establishments that already participated in the previous round of the ES. While it is expected that drop-out rates will be kept to a minimum, it is also clear that some establishments may refuse or be unable to participate in the present round of surveys. Those establishments that choose not to participate will be replaced with other establishments. To preserve the original sample design, an establishment that refuses to participate will be replaced by another with the same characteristics, following the preference order provided by the TTL. Deviations from this protocol must be authorized by the TTL.

The WB will provide the full list of panel firms from the previous round of surveys. Regardless of whether this firm is selected for an interview, the Vendor will be required to contact all the panel firms to determine their current operating status (see section 3.5.8) and generate a full status report of the prior ES wave. This is a deliverable of the project.

3.5.2 Recruitment

Since high non-participation rates could jeopardize the success of the project and can bias estimates based on the data collected, special emphasis must be put into designing and implementing a plan to contact and

recruit selected firms to participate. The Vendor is responsible for writing, getting approval of, and sending letters and/or emails, making phone calls, setting appointments, and making attempts to secure high levels of participation. Experience shows that Vendors, who have limited experience conducting establishment-level surveys, often underestimate the resources required and needed for the screening and recruitment of prospective survey respondents.

A formal approach when contacting the prospective respondents selected for interviews has proven to be the best method given the sensitive nature of the information requested and the burden that the interview represents for busy senior managers. The Vendor should expect and prepare for this responsibility and allocate the resources required for a well-planned and well-executed recruitment campaign. In the process of recruitment, the vendor should abide by the ethical standards of informed consent, which may be requested orally. This entails providing prospective respondents with 1) the description and purpose of the survey project, 2) the expectations of respondent in terms of time commitment (how long the interview will take), 3) an overview of how the collected information and data will be used and analyzed, 4) how respondents' individual data are kept confidential, and 5) how to redress any concerns about the study.

The Vendor will be required to work with local business associations and similar institutions to ensure broad-based participation in the survey, to facilitate access to the senior managers, and to maximize participation and response rates to each question. Most importantly, in countries where the objective is to interview firms included in the previous rounds of the ES, the Vendor must design and implement a strong campaign to encourage the establishments included in the previous rounds of the ES to participate again.

3.5.3 GPS Coordinates of the Interviewed Establishments

During fieldwork, it is required to record the Global Positioning System (GPS) coordinates of each establishment. The GPS coordinates should capture geo-spatial location of the establishment being interviewed, which may differ from the place where the interview takes place. If the interview is conducted through videoconferencing, or GPS is not collected during the interview for any other reason, the location of the establishment must be found on a map, transformed to GPS coordinates, and included in the dataset.

3.5.4 Email Addresses

The selected Vendor is expected to collect and verify email addresses of all interviewed establishments. Email addresses of the establishment itself are preferred over the email addresses of individuals who work at the establishment. It is important that the Vendor verifies the email addresses, either through sending a follow-up thank you email, or other tools of email address verification. In case of invalid emails, the Vendor is expected to provide corrected email addresses. The collection of email addresses is essential for successful distribution of the Country Profiles and for future survey waves for the construction of panel datasets.

3.5.5 Training

The Vendor must have a well-developed plan to thoroughly train their fieldwork supervisors, enumerators and the data quality staff on the questionnaire and survey procedures. Enumerators must be able to interpret all questions consistently and ask all questions in the prescribed manner. All supervisors and enumerators are expected to read, study, and understand the Questionnaire Manual.

Supervisors and enumerators should preferably have previous experience in survey implementation, should be available throughout the entire duration of the fieldwork, and ideally have some knowledge of accounting and/or finance; some familiarity with the survey topics facilitates the detection of

inconsistencies and misunderstandings. The selected Vendor needs to take into account that given the characteristics and number of survey respondents, careful planning of the size and composition of the fieldwork team is required as a typical enumerator cannot expect to complete more than 2 interviews per day and, depending on the efficiency of the process to make appointments, there may be days with low productivity. The experience in previous surveys shows that the process of making appointments with selected firms requires considerable time and effort.

Training of enumerators and supervisors in the specific implementation of the questionnaire is essential for the success of the project. For this reason, Vendors are encouraged to plan at least one training session with each local team, ideally in their own country. The TTL and/or other staff of the Enterprise Analysis Unit (possibly two people or more) will be part of these training sessions. However, it is the Vendor's responsibility to be able to independently train all the staff participating in the survey implementation.

Experience shows that a full training session requires up to four business days. This should include extensive training on the CAPI script. Trainings should ideally be conducted following the receipt and approval of cleaned sampling frames in the relevant country, to allow for the timely launch of fieldwork shortly thereafter.

3.5.6 Piloting

Immediately after the training and before the actual survey fieldwork, the Vendor must pilot the questionnaires on a selection of 10-15 establishments in each country. The purpose of piloting is to ensure that the questionnaire translation is correct, and that the questions are appropriately phrased for the local environment. The pilot will also test the CAPI script. In addition, these interviews must be timed to ascertain the length of implementing the questionnaire. The Vendor must immediately report to the TTL any issues that arise during piloting.

All modifications to the questionnaires, CAPI script, instructions and sampling framework that may be suggested from the piloting results must be approved by the TTL. Any changes to the format or ordering of the questionnaire to facilitate implementation must also be cleared with the TTL.

3.5.7 Interviewing

After training the fieldwork team, after the results are obtained from piloting, and after the final questionnaires and CAPI script have been approved by the TTL, only then should survey fieldwork commence.

The completion of survey fieldwork is determined by the TTL by taking into consideration the number of completed interviews and the quality and comprehensiveness of the data gathered from these interviews. For a survey to be considered complete, the large majority of the relevant information, including the accounting data, must be obtained and entered into the dataset. No questions should be left blank except the ones skipped due to correctly applied skip patterns. The integrity and accuracy of the data is vital. The Vendor will establish procedures to check the quality of the interviews. A minimum of 10% of the completed interviews will be required to be back-checked by telephone by the Vendor to ensure integrity of the data collection. Additional call-backs may be required depending on the quality control feedback provided by the WB. Supervisors of the survey will randomly check enumerators and accompany interviewers on some interviews. Representatives of the WB may accompany survey teams to monitor effectiveness, ensure quality and check for progress in the field.

The Contactor will develop procedures for compliant processing and timely deletion of personal data.

3.5.8 Non-Participation and the Progress Report

The Vendor must maximize efforts to reduce non-participation rates. To keep track of this and to separate non-participation from sampling frame problems, a weekly Progress Report will be submitted to the TTL. The Progress Report will be based on a template provided by the WB. The Vendor will be required to fill in the template with the required information necessary to monitor the survey progress and send an up-to-date copy to the TTL at least once each week.

Every establishment contacted during fieldwork must be classified according to specific codes provided in the template (see table in Appendix III).

A separate report will have to be prepared for all panel firms, independently of whether they will be interviewed or not. The Vendor will be required to attempt to contact all establishments from the previous survey wave to determine each establishment's current operating status (see section 3.5.1). The outcome of this effort will be provided in a separate report providing a code for each establishment following the same codes in the weekly Progress Report, including those that have ceased operations. The purpose of the report is to have clear description of the status of each establishment interviewed in the previous survey wave. Consequently, whenever an establishment is not located, special efforts should be made to find out what happened since the last interview to differentiate whether the establishment disappeared, moved, was purchased by other firm or any other case.

3.5.9 Staff

It is important that the Vendor puts in place mechanisms to guarantee low rotation of personnel.

Team members will have the following duties:

- The duties of the **enumerator** will be: to visit the selected establishments and ensure their participation; to conduct face-to-face interviews with the selected respondents or through video-conference, where applicable; to ensure completeness and accuracy of respondents' answers; to deliver completed interviews to supervisors; and to safeguard the confidentiality and privacy of the collected information.

- The duties of the **supervisors** will be: to supervise all activities of their assigned enumerators during the data collection process through spot checks and call backs; to assess the quality of the work of the enumerators and the quality of the data from the completed questionnaire; to approve completed questionnaires; to assist enumerators in securing establishments' participation if necessary; and to provide feedback to enumerators on quality assurance and methodology requirements.

- A **project coordinator** will oversee the fieldwork. The duties of the project coordinator will be: to supervise all activities of supervisors and enumerators; to coordinate the selection of establishments and the screening process to ensure that selected establishments meet the requirements of the study; to assign establishments to be surveyed to supervisors and enumerators; to assist the team to ensure maximum participation and minimize nonresponse; to coordinate with supervisors/enumerators the quality control of the data collection process; and to comply with the policies and procedures for the collection, safekeeping, processing, management and deletion of personal data in accordance with the Vendor's obligations under the Data Protection Annex (Annex 1).

In case any person involved in the data collection must be permanently or temporarily replaced during the duration of the study, the Vendor will ensure sound knowledge transfer and training and inform the TTL no later than 7 business days after the change; such knowledge transfer includes all relevant data and

materials. In case of replacement of key personnel, i.e., project coordinators, regional managers, regional supervisors, IT manager or subcontractor, the proposed replacement will be approved first by the TTL. If necessary, the WB TTL may request re-training of the Vendor's staff involved in the project.

At the outset of the project, the Vendor should provide a staffing plan to the TTL.

3.5.10 Subcontracting

Vendors intending to subcontract fieldwork operations must present the names and references of all the proposed subcontractors. The WB reserves the right of approving each subcontractor. Any change of the subcontractors must be accepted by the TTL in advance. Vendors are encouraged to include sufficient information on the subcontractors for the selection committee to decide on their eligibility to carry out WB work and their ability to carry out the survey in each country. Vendors must be able to accommodate alternative subcontractors whenever the TTL and the conditions of the country determine it to be necessary.

If personal data is being collected by or shared with the subcontractors, the primary Vendor is expressly responsible for the subcontractors meeting our confidentiality and data protection requirements.

3.5.11 Potential Changes to Survey Design

In unforeseen circumstances, beyond the control of the WB or the Vendor occur, such that the fieldwork in a country or region may be significantly delayed, the WB reserves the right to change the survey design. This may include adjusting the target number of interviews, or from region A to region B within Spain. The TTL will discuss with the Vendor the most efficient way to implement such changes.

3.5.12 Data Deliveries

The survey data will be delivered to the WB in STATA or SPSS electronic format. In case the Vendor prefers to submit data in alternative formats, this will first be approved by the TTL. The final format of each variable in the dataset will follow the guidelines defined by the global codebook, provided by the WB. All data deliveries will take place through a secured server provided by the WB TTL (OneDrive).

The Vendor will provide the collected data at any time following a request by the TTL, and also at three predefined stages during the data gathering/entry process for consistency check and quality control. The first set will be delivered after ten percent (10%) of the total number of interviews have been completed. The second set will be delivered after fifty percent (50%) of the total number of interviews have been completed. The final set will be delivered after completion of one hundred percent (100%) of the interviews. Each delivery should include translated and verified values for string variables to enable WB review.

The TTL may request more frequent data deliveries in addition to the three main deliveries. The WB will check the data and provide feedback to the Vendor on any errors or inconsistencies.

Confidentiality and Data Ownership:

The Vendor will protect the confidentiality of the data provided by establishments and individuals participating in the survey at all stages. All collected data (excluding any personal data which may be collected by the Vendor for business processes such as making call-backs to respondents), including the sampling frame (if it is assembled by the Vendor for this project), is confidential and is the sole property of the WB. Its purpose is to support research on the business environment and the development of the private sector.

No data or other information from this survey will be released to third parties without the written approval of the WB. The Vendor will turn over all data (excluding the personal information collected for the purposes of quality control), questionnaires and other material to the WB and will not retain any information or material after the survey data collection has ended. **The names of participating establishments and the GPS coordinates of the establishments will not be released by the Vendor to any other party for any reason.**

3.5.13 Country Profiles Distribution

The WB will provide two versions of the Country Profile. The first version will be based on the previous round of the surveys and will be distributed during the fieldwork as a promotional tool (pre-survey Country Profile). The second version will use the data generated during the current round of the survey (post-survey Country Profile). If any changes are made to the text of the second version of the Country Profile, the Vendor might be required to translate this new text into the local language. The post-survey Country Profile will be distributed, by the Vendor, to all interviewed establishments via email (in PDF form, as generated by the WB). The Vendor will provide a short report detailing email delivery of Country Profiles to all interviewed establishments. If valid email addresses are not available, the WB and the Vendor will jointly determine the most efficient and economical way to deliver the Country Profile to the respondents who lack email addresses.

3.5.14 Business Continuity plan

Vendors are requested to submit to the WB, a business continuity plan detailing how they will continue performance of this Contract with a minimum of delay, interruption or other disruption in the event of a security or health and safety event which affects the Vendor's ability to perform the services.

The Vendor will maintain a comprehensive business continuity plan and will provide an executive summary of such plan upon request by the WB. The Vendor will test the adequacy of its business continuity plan at least annually and upon request, the WB may participate in such tests. Upon request by the WB, the Vendor will provide the WB with a letter stating the most recent business continuity test results. In the event of a business disruption that impacts the Vendor's provision of the Services, the Vendor will promptly notify the WB of the disruption and the steps being implemented under the business continuity plan.

3.6 Supplementary Tasks

Data collected with the Enterprise Surveys will be a source of information for the World Bank's Business Ready (B-READY) project. The B-READY project will provide quantitative benchmarking of the business environment across economies around the world, with annual frequency and for most economies worldwide.

Data collection for B-READY will be undertaken through expert consultations, and remuneration will be provided to such experts. It is expected that around 22 topic questionnaires will be used to measure the business environment and will be administered to 4 experts per questionnaire in the country. Each expert will receive remuneration of approximately USD 400 per topic questionnaire, as compensation for their services provided. In addition to implementing the Enterprise Survey, the remuneration of these experts (henceforth referred to as "expert payments") will also be managed by the Vendor. In order to do so, the Vendor will first contact the list of experts, which will be provided by the World Bank, to obtain the details of their desired mode of receiving the remuneration (i.e. bank transfer or other modes), and all necessary details required to undertake the transfer of funds such as whether the expert would be paid as a legal person charging a value added tax (VAT) or as a natural person. These reimbursable expert payments

should be paid each year in September 2024, in September 2025, and in September 2026, which will be the last task of the contract. The World Bank will provide the funds to make such expert payments.

The Vendor will make these expert payments upon successful completion of the expert consultation, which will be determined by the World Bank. That is, the Vendor is not responsible for the completion (or quality) of the expert consultation, but only for arranging the transfer of funds to each expert within a prescribed time frame. The Vendor will maintain detailed records of expert payment transactions and provide a report to the TTL upon successful completion of the expert payments. Keeping personal data on individuals (name, contact information and payment details such as bank account) is needed by the Vendor for a limited period. When collecting and processing personal data, the Vendor must fulfill its obligations as outlined in the Data Protection Annex (Annex 1), and in the Information Security for Contractors Policy (Annex 2).

4. Deliverables

The Vendor:

a. Will provide tables with the universe population figures in the Spain ES. The tables will summarize the total number of establishments that are in a specified location, size, and business sector (see table in Appendix I).
b. Will provide World Bank TTL a plan detailing outreach and recruitment plans for engaging with business associations and maximizing survey participation.
c. Will check the translations of all local languages of each economy that will be used in the fieldwork the following documents: Screener and Enterprise Survey questionnaires, the Questionnaire Manual, the informed consent document, the Country Profile (both the pre-survey and post-survey versions), and all training materials (presentations, tip sheet, letters of invitation, etc.).
d. Will train all enumerators on the survey methodology and questionnaire material.
e. Will pilot the survey questionnaire on 10-15 establishments in each economy prior to launching the surveys. Will provide the pilot data and pilot report to the TTL.
f. Will confirm with the TTL any necessary or suggested changes on the questionnaires based on the results of piloting the surveys.
g. Will conduct survey interviews, using the samples approved by the TTL, via CAPI or other approved modes of data collection.
h. Will provide weekly Progress Reports that include eligibility and interview status information for all contacted establishments, in a format approved by the TTL.
i. Will provide Vendor staffing reports noting any changes in staffing including managers, supervisors, and enumerators.
j. Will ensure that data deliveries comply with global codebook restrictions on out-of-range values. Data deliveries must meet the quality control standards provided by the TTL, these include correcting inconsistencies, avoiding missingness wherever possible., and incorporating data obtained from post-interview call-backs of respondents.
k. Will provide the survey data to the WB, for quality control checks at the request of the TTL and when the following milestones are reached: ten percent (10%) of the overall number of interviews; fifty percent (50%) of the overall number of interviews; and after completion of one hundred percent (100%) of the interviews.
l. Will translate answers of open-ended questions into English (to be made available at the time of each data delivery) and if necessary, rewrite them as per instructions provided by the TTL. The Vendor is responsible for providing to the TTL, open-ended text responses that meet the level of detail and quality guidelines provided by the WB.

m. Will provide the WB with a clean, English-labelled dataset comprised of 1,440 completed Spain ES 2024 interviews. The data will be a STATA or SPSS electronic dataset. The dataset will contain all variables included in the questionnaires. Each establishment shall have a unique numeric identifier.

n. Will provide the WB with a second dataset for Spain ES 2024 including the up-to-date location information of each interviewed establishment: name, address, GPS coordinates, phone number, email/web address. Each establishment will have a unique alpha code identifier that enables one-to-one matching of the establishments that appear in both datasets. Aside from respondent's contact information, no personal data shall be provided to the WB. Personal data must be destroyed after a maximum period of 12 months after the completion of the project.

o. Will provide WB a report on the operating status of all panel firms (previously interviewed establishments). The report should indicate that all panel firms have been contacted and their eligibility status.

p. Will prepare an Implementation Report, in English, which includes pertinent information for researchers. The report will cover challenges encountered during the survey project, any possible biases which were introduced during survey fieldwork, and the fieldwork methodology and tools employed. Any data changed or removed in the "cleaning" process other than through clarification with the survey respondents will also be reported.

q. Will distribute the Country Profiles to all interviewed establishments after the fieldwork is finished and after the WB has generated this post-survey document. The Vendor can distribute the Country Profiles via email, using the email addresses of establishments collected during the fieldwork. The Vendor will provide a short report detailing email delivery of Country Profiles to all interviewed establishments. If valid email addresses are not available, the WB and the Vendor will work together to find the most efficient and economical way to deliver the Country Profile to these firms. The WB will check whether the Country Profiles have been delivered to interviewed establishments by re-contacting a randomly selected sub-sample of interviewed establishments to verify. If the delivery rate is below 80%, payment will be reduced as indicated in the Payment Schedule of this ToR.

r. For administering the remuneration for B-READY experts, will contact a WB-provided list of experts for the country and obtain from them details of their desired mode of payment of remuneration (e.g. bank transfer), and all necessary details required to undertake the transfer of funds. These payments will be executed in 2024, 2025 and 2026.

s. Upon notification from the WB that the B-READY experts should be paid, the Vendor will make the expert payments within the prescribed time frame, will maintain detailed records of these payment transactions, and will provide a report to the WB on the status of each expert payment.

t. Will be responsible for protecting confidentiality of Enterprise Surveys data and B-READY expert payments data.

5. Terms and Conditions

The contract for this service shall be subject to the World Bank Contract Terms and Conditions for Consulting Services (T&Cs), copy available at https://thedocs.worldbank.org/en/doc/f9fd931b1d771033773ea466e82ed5eb-0180012023/original/WBG-Terms-and-Conditions-Consulting-Services-English-2023.pdf.

In addition to the T&Cs above, the contract shall also be subject to the following:

- World Bank Information Security Policy for Vendors, copy available at https://thedocs.worldbank.org/en/doc/448151490189823243-0180022017/original/InformationSecurityPolicyforVendors.pdf.

- World Bank Policy on Access to Information, copy available at https://ppfdocuments.azureedge.net/3693.pdf

The Vendor has to share their Third Party Risk Management Framework (TPRMF). If there is personal data being shared with subcontractors, the Vendor ensures obligations will be flown down to subcontractors and the Vendor is expressly responsible for subcontractors meeting our confidentiality and privacy requirements.

6. Tentative Time Schedule

The timeline of the assignment is as follows. Upon signing the contract, the implementing Vendor will carry out the logistical preparation for the Enterprise Survey in order to train interviewers as soon as possible. If translation services are required, this activity should take place as soon as the finalized questionnaire and training materials are provided by the TTL to the Vendor. Similarly, any activities regarding the sampling frame should commence immediately.

Survey fieldwork is expected to start by November 2023. The implementing Vendor is expected to submit the completed, clean dataset and all other deliverables including the final implementation report to the WB by September 2024.

7. Payment schedule

An initial payment of five percent (5%) of the total contract value, excluding the reimbursable payment of experts, will be made upon signing of the contract and delivery of the preliminary logistical work (training plan, staffing plan, outreach and recruitment plan, and sampling frame strategy).

A payment of five percent (5%) of the total contract value, excluding the reimbursable payment of experts, will be made upon delivery of the translated questionnaire and training materials and completion of the training for the enumerators on the survey methodology.

A payment of twenty percent (20%) of the value of the contract, excluding the reimbursable payment of experts, will be paid upon receipt of the first ten percent (10%) of data and approval by the TTL that the data delivery meets the requirements of the ToR.

A payment of twenty-five percent (25%) of the value of the contract, excluding the reimbursable payment of experts, will be paid upon receipt of the first fifty percent (50%) of data and approval by the TTL that the data delivery meets the requirements of the ToR.

A payment of maximum twenty percent (20%) of the value of the contract, excluding the reimbursable payment of experts, will be paid on a prorated basis only if Vendor has submitted 80% or more of the ES data. As an example, if 85% or 95% of the ES data is delivered by September 30, 2024, a payment in the amount of 5% or 15%, respectively will be due to the Vendor. If Vendor delivers less than 80% of the ES data by September 30, 2024, no payment will be due to the Vendor.

A payment of twenty-five percent of the value of the contract (25%) of the value of the contract, excluding the reimbursable payment of experts, will be made upon receipt and approval by the TTL of the final dataset, the Implementation Report, and remaining project deliverables.

A payment for the completion of payments to B-READY experts will be made by **September 30th, 2024**. This payment will be approximately $35,200 plus associated (reimbursable) management fees; however, this payment will be lower if fewer B-READY experts need to be paid. The Vendor will provide to the TTL proof that the payments to B-READY experts were completed.

A payment for the completion of payments to B-READY experts will be made by **September 30th, 2025**. This payment will be approximately $35,200 plus associated (reimbursable) management fees; however, this payment will be lower if fewer B-READY experts need to be paid. The Vendor will provide to the TTL proof that the payments to B-READY experts were completed.

A payment for the completion of payments to B-READY experts will be made by **September 30th, 2026**. This payment will be approximately $35,200 plus associated (reimbursable) management fees; however, this payment will be lower if fewer B-READY experts need to be paid. The Vendor will provide to the TTL proof that the payments to B-READY experts were completed.

APPENDIX I : UNIVERSE POPULATION TABLE FORMAT

Number of active establishments		Manufacturing – category 1	Manufacturing – category 2	Rest of Manufacturing – category 3	Services – category 1, Retail	Services – category 2	Rest of Services – category 3
Location 1	Small (5-19) employees						
	Medium (20-99) employees						
	Large (100+) employees						
Location 2	Small (5-19) employees						
	Medium (20-99) employees						
	Large (100+) employees						
Location 3	Small (5-19) employees						
	Medium (20-99) employees						
	Large (100+) employees						

Note: the number of manufacturing and location strata categories are subject to sample size restrictions depending on the survey budget and size of the economy (the greater the budget and size of the economy, the larger number of locations and sectors singled out for stratification).

SOURCE: should be the most complete, and up-to-date estimate of the total number of establishments, satisfying the eligibility criteria as outlined in section 3.1.

APPENDIX II: SAMPLING FRAME TEMPLATE

Sampling frames should include only active and registered establishments. They should exclude co-operatives. Vendor should note the level of aggregation of sampling frames, which should be at the level of the establishment. If establishment-level frames are not available, specific accommodations will be made.

Establishment unique ID number	Location	ISIC 3.1 or 4.0 Code	Number of Employees	Establishment name	Address	City, Region/Province	Phone	Email

SOURCE: *NAME OF SOURCE* (YEAR)

Note that the source should be the most updated recent list available in each country.

APPENDIX III: ELIGIBILITY AND STATUS CODES

Eligibility status
ELIGIBLES
1. Eligible establishment (Correct name and address)
2. Eligible establishment (Different name but same address - the new firm/establishment bought the original firm/establishment)
3. Eligible establishment (Different name but same address - the firm/establishment changed its name)
4. Eligible establishment (Moved and traced)
16. Panel establishment with less than 5 employees (still eligible for interview!)
INELIGIBLE
5. The establishment has less than 5 permanent full-time employees
616. The establishment has less than 5 permanent full-time employees
618. The firm/establishment discontinued businesses - (Original establishment disappeared and is now a different firm)
619. The firm/establishment discontinued businesses - (Establishment was bought out by another firm)
620. The firm/establishment discontinued businesses - (It was impossible to determine for what reason)
621. The firm/establishment discontinued businesses - (Other)
71. Ineligible legal status: not a business, but private household
72. Ineligible legal status: cooperatives, non-profit organizations, etc.
8. Ineligible activity: Education, Agriculture, Finances, Government, etc.
OUT OF TARGET
151. Out of target - outside the covered regions
152. Out of target - moved abroad
153. Out of target - Not registered with Statistical Authority
154. Out of target - establishment is HQ without production or sales of goods or services
155. Out of target - establishment was not in operation for the entirety of last fiscal year

156. Duplicated firm/establishment within the sample

UNOBTAINABLE

91. No reply after having called in different days of the week and in different business hours
92. Line out of order
93. No tone
94. Phone number does not exist
10. Answering machine
11. Fax line- data line
12. Wrong address/ moved away and could not get the new references

SCREENER REFUSAL

13. Refuses to answer the Screener (includes if the person just hangs up without talking to the recruiter)

IN PROCESS

14. In process (the establishment is being called/ is being contacted - previous to ask the Screener)

Interview status
1. Complete effective interviews 2. Incomplete effective interviews 3. Refusal 4. In process to make an appointment (they have already answered the Screener)

Refusal reasons
Only use if the /establishment has agreed to participate during the Screener! (For refusal during the Screener use code 13 in Status code) 1. Does not want to participate 2. Has no time to participate 3. Away from town/ traveling 4. Not interested in the subject

5. Do not answer any surveys as a general rule for the firm/establishment
6. Other

Annex 1 – Data Protection Annex

1. The Contract

1.01 This Data Protection Annex is incorporated into, forms part of, and is subject to the terms and conditions of the Contract.

1.02 Any capitalized term used but not defined in this Data Protection Annex has the meaning given to it in the Contract.

2. Confidentiality and Compliance with Applicable Law

2.01 Purchaser Data comprises Purchaser's confidential information and is subject to all protections and obligations applicable to Purchaser's confidential information under the Contract.

2.02 Vendor will comply with all applicable data privacy, data security, and other data protection related laws, regulations or directives in connection with the performance of its obligations under the Contract.

3. Custodian of Purchaser Data and Use of Purchaser Data

3.01 Vendor is a custodian only of Purchaser Data and accordingly:

(a) the Contract does not create any right or license for Vendor or any third parties to use any Purchaser Data for their own benefit or for the benefit of any person or entity other than Purchaser,

(b) as between Purchaser and Vendor, Purchaser is the sole and exclusive owner of, and will retain all right, title, and interest in and to any Purchaser Data,

(c) regardless of the medium or form in which Purchaser Data is stored Vendor will not acquire or assert any right in, title to, or encumbrance over, any Purchaser Data for any reason,

(d) Vendor will not, under any circumstances, sell, assign, lease, license, securitize, otherwise commercially exploit any Purchaser Data,

(e) Vendor will not directly or indirectly disclose, transmit or otherwise provide access to Purchaser Data to any person or entity other than Authorized Personnel without Purchaser's prior written consent in each and every instance,

(f) Vendor will only Process, or permit Processing of, Purchaser Data solely and exclusively for the Permitted Purpose and only for so long as is required to fulfill the Permitted Purpose and not for any other Purpose, and

(g) Purchaser has the right to retrieve or delete, or require the retrieval or deletion of, any Purchaser Data at any time and Vendor will promptly comply, and cause any Subprocessors to comply, with a Purchaser request for retrieval or deletion of any Purchaser Data.

3.02 Vendor will not, unless expressly authorized to do so under the Contract: (a) track, store, analyze, distribute, disclose, sell, license, or otherwise transfer to any third party any user data

(e.g., internet browser type, version, system specifications, access logs, IP address, MAC address) relating to Purchaser or captured by Vendor in the course of performing its obligations under the Contract and (b) target advertisements, promotions, offers, or other marketing based on user data relating to Purchaser or captured by Vendor in the course of performing its obligations under this Contract.

3.03 To the extent Vendor relies on artificial intelligence or machine learning systems in connection with providing services to the Purchaser or to Process Purchaser Data, Vendor will use its best efforts to ensure that (a) the results of any such systems will not be deceptive or misleading, and (b) such systems will be free of bias and discrimination, including as defined by industry standards and applicable law. Vendor will periodically review such systems and maintain them in accordance with industry standards and provide updates on such effort to the Purchaser at the Purchaser's request.

4. Archival and Other Immunities

4.01 Vendor agrees that Purchaser Data:

(a) are official archives of the relevant member of the World Bank Group, used to perform its core function,

(b) constitute the "archives" and "property" of the relevant member of the World Bank Group pursuant to applicable treaties and under applicable international and domestic laws, and

(c) are inviolable and subject to absolute and full immunity from legal and judicial process, search, seizure, confiscation, attachment, and discovery by others as set forth in such treaties and laws.

4.02 Vendor will take such actions as are requested by Purchaser from time to time to protect the World Bank Group's archives and to preserve the World Bank Group's privileges and immunities.

4.03 Vendor agrees that none of:

(a) Purchaser's execution or performance of the Contract,

(b) Purchaser providing any Purchaser Data to Vendor or any third parties in connection with the Contract, or

(c) Purchaser requiring Vendor or any of its representatives to perform any obligations under the Contract,

will be construed as any member of the World Bank Group waiving, renouncing, modifying, or intending to waive, renounce, or modify, to any extent or in any manner whatsoever, any privileges or immunities under any treaty, international law, or domestics law, which privileges and immunities are specifically reserved.

5. Third Party Data Requests

5.01 In the event of a Third Party Data Request, Vendor will, unless expressly prohibited by law:

(a) immediately notify Purchaser of the existence of the Third Party Data Request,

(b) use its best efforts to redirect the third party to Purchaser,

(c) refrain from disclosing or providing access to any Purchaser Data in response to the Third Party Request without first obtaining Purchaser's prior and express written consent,

(d) provide Purchaser with sole and exclusive control over any response to the Third Party Data Request, including without limitation the sole and exclusive right to initiate or respond to any legal proceedings, in so far it affects any Purchaser Data, and

(e) take such actions as are reasonably requested by Purchaser to help protect Purchaser Data, including without limitation by initiating or responding to legal proceedings, at Purchaser's request.

5.02 If, notwithstanding the above, Vendor remains compelled by applicable law to disclose or provide the third party with access to any Purchaser Data, Vendor will only disclose that portion of the Purchaser Data that is strictly required to discharge its obligations under applicable law and will use best efforts to ensure that the Purchaser Data is afforded appropriate protection.

6. Data Security Safeguards

6.01 Vendor will implement and, at all times maintain, administrative, physical, technical, and organizational safeguards appropriate to the risk represented by the nature of the Purchaser Data and the Processing permitted under the Contract.

6.02 In addition, Vendor will, at a minimum:

(a) maintain all safeguards to a standard equivalent to, or more stringent than, the standards specified in ISO 27001 and SSAE 18 SOC 2 Type II,

(b) encrypt all Purchaser Data at rest, including any backup, and in transit (using TLS 1.2 or later), including via any web interface, at all times at a level that is equivalent to, or stronger than, 256-bit AES or 2048-bit RSA, and hash all passwords, and otherwise perform all hashing operations, using SHA-256 or stronger,

(c) treat any and all information relating to Purchaser's remote access and transmission protocols as Purchaser's confidential information in accordance with the Contract,

(d) take all necessary steps to maintain the integrity of Purchaser Data and to protect it against deterioration and degradation of its quality and authenticity, and

(e) ensure that its employees attend regular cybersecurity trainings.

6.03 Vendor will make daily backup copies of Purchaser Data and store such backup copies in an immutable, encrypted, machine-readable, and widely portable format for a minimum period of ninety (90) days. Vendor will store such backup copies of Purchaser Data offline or on a separate network and will test such backup copies of Purchaser Data on a regular basis. Vendor will, at Purchaser's request, provide Purchaser with all such backup copies of Purchaser Data.

6.04 Vendor will implement, maintain, and update as necessary, reasonable and industry-recognized user access rules for users accessing Purchaser Data based on the need to know and

the principle of least privilege, including user ID and password requirements, session timeout and re- authentication requirements, unsuccessful login attempt limits, privileged access limits, multifactor authentication at Purchaser's reasonable request, and a system for tracking and enforcing requests, updates and the termination of access rights.

6.05 Vendor will, at Purchaser's request, (a) provide a complete software bill of material ("SBOM") containing the minimum elements as defined by current industry guidance, standard or regulation for the supported life of software products provided under this Contract, (b) monitor for security vulnerabilities in the software components listed in the SBOM, and (c) use a risk-based approach to mitigate in a timely manner any known exploitable vulnerabilities in the software components included in the SBOM or such other software components as may otherwise Process Purchaser Data. Vendor will ensure that software components in the SBOM is actively maintained. In the event a software component in the SBOM ceases to be actively maintained, Vendor will notify Purchaser and either replace the software component with an actively maintained equivalent or assume active maintenance internally of the software component. In the event the maintainer of a software component in the SBOM changes to a new maintainer, Vendor will notify Purchaser and perform thorough cybersecurity testing of any subsequent releases of the software component before placing new versions into active use.

7. Data Security Testing

7.01 Vendor will, at its own expense, conduct or have conducted the following at least once per year and immediately after any Data Incident:

(a) an SSAE 18 SOC 2 Type II audit of Vendor's security policies, procedures, and controls,

(b) a certification under ISO 27001,

(c) a vulnerability scan, performed by a third-party scanner approved by Purchaser, of Vendor's systems, networks, and facilities that are used in performance of the Contract, and

(d) a formal penetration test, performed by qualified personnel approved by Purchaser, of Vendor's systems, networks, and facilities that are used in performance of the Contract.

7.02 Vendor will, at Purchaser's request, provide documentation evidencing the results of the audits, certifications, scans, and tests required under Section 7.01.

7.03 If the above audits, certifications, scans and tests reveal any vulnerabilities, weaknesses, or areas of non-compliance, Vendor will, within thirty (30) days, take any remedial steps necessary to address such issues to ensure full compliance with its obligations under this Data Protection Annex. Vendor will keep Purchaser informed of the status of any such remedial action, including the estimated timetable, and will promptly provide Purchaser with written documentation certifying completion of the remedial action.

8. Data Protection Audit and Inquiries

8.01 Purchaser, or an independent auditor appointed by Purchaser, has the right to conduct an audit of Vendor's, and any Subprocessor's, data protection practices to verify compliance with the obligations under this Data Protection Annex once per year, or at any time after a Data Incident, upon prior written notice.

8.02 Vendor will take all reasonable steps to, and will cause all Subprocessors to, cooperate with any such audit, including without limitation, by making available any relevant records, policies, systems or facilities, and granting access to any premises or personnel, involved in or used for the performance of any data-related obligations under the Contract.

8.03 Vendor will, at Purchaser's request, provide (a) timely and complete responses to Purchaser's cybersecurity inquiries related to procedural and technical controls that Vendor has implemented to protect against emerging and current cybersecurity threats, including ransomware attacks and software supply chain vulnerabilities, and (b) details on the actions that Vendor has taken or plans to take in order to remediate specified vulnerabilities.

9. Geographic Location of Purchaser Data

9.01 Vendor will and will cause any Subprocessor to: (a) only store Purchaser Data at facilities located within the United States, Canada, or the United Kingdom, and (b) provide Purchaser with prior written notice of the location of any facilities which will be used to store Purchaser Data.

10. Security Information and Event Management

10.01 Vendor will have and maintain a security information and event management system ("SIEM") to detect and log all activity which may indicate unauthorized access, unauthorized use, or an unauthorized attempt to compromise Vendor's security safeguards for any systems or facilities used to Process, host, or store Purchaser Data.

10.02 Vendor's SIEM will have the capacity to provide information on an automated and immediate basis to a designated Purchaser system and Vendor will cause its SIEM to provide such information to Purchaser's designated system upon request.

Data Incident

10.03 If Vendor becomes aware of a Data Incident, Vendor will:

(a) immediately, but in any event within 24 hours, notify Purchaser,

(b) take all necessary steps to investigate, contain and mitigate the Data Incident and to restore normal functionality,

(c) cooperate with Purchaser's requests for information and assistance, including without limitation, by providing Purchaser with periodic written updates regarding the Data Incident and Vendor's response to the Data Incident,

(d) at Purchaser's request, prepare and send any notifications required under applicable law arising from the Data Incident,

(e) at Purchaser's request, cooperate with Purchaser with respect to any action by any regulatory body or any lawsuit arising from the Data Incident, and

(f) as soon as reasonably practicable, review Vendor's response to the Data Incident to identify and address any vulnerabilities, weaknesses or failures in Vendor's response processes and report all planned and completed remediations to Purchaser.

10.04 Vendor acknowledges that a Data Incident may cause irreparable harm to Purchaser, other members of the World Bank Group, and third parties, for which monetary damages may be an inadequate remedy.

10.05 Vendor will indemnify and hold harmless Purchaser from any and all liabilities arising out of or in connection with a Data Incident.

11. Cyber and Privacy Insurance

11.01 Vendor will maintain, at its own cost, cyber and privacy insurance coverage providing protection and reimbursement against liability for a Data Incident, including fees or other compensation paid to any person or entity related to investigating, mitigating, and remediating a Data Incident, and for notifying, and providing identity theft and credit monitoring services to any persons or entities affected by a Data Incident, with a limit of at least USD 1 million per occurrence.

11.02 Vendor will, upon request, provide Purchaser with a certificate of insurance for the coverage required hereunder. Vendor will not cancel, fail to renew or materially alter such insurance coverage without at least thirty (30) days prior written notice to Purchaser.

12. Return or Destruction of Purchaser Data

12.01 Upon termination or expiration of the Contract, Vendor will at Purchaser's request: (a) return Purchaser Data to Purchaser by transmitting Purchaser Data in a widely supported, commonly used and machine-readable format, and in a secure and encrypted manner, and/or (b) delete or destroy Purchaser Data by rendering Purchaser Data permanently unusable, unreadable, or indecipherable using industry standard measures.

12.02 If Purchaser does not request the return and/or deletion of Purchaser Data under Section 13.01 within one (1) year of termination or expiration of the Contract, Vendor will immediately delete or destroy Purchaser Data in accordance with Section 13.01(b).

12.03 Vendor will, at Purchaser's request, provide Purchaser with written certification from a duly authorized officer attesting to Vendor's compliance with Sections 13.01 and 13.02, the date of the return, destruction or deletion of Purchaser Data and the methods used for such destruction or deletion.

12.04 Notwithstanding the above, Vendor may retain Purchaser Data to the extent necessary for Vendor to comply with applicable law or Vendor's own mandatory record keeping policies, provided that, in each case, Vendor: (a) only retains Purchaser Data for the minimum period necessary to satisfy any such obligations, (b) notifies Purchaser of the duration of the retention period in writing, and (c) remains bound by all obligations in the Contract with respect to the retained Purchaser Data.

13. Personal Data

13.01 In the course of performing the Contract, Vendor may be required to Process Personal Data on behalf of Purchaser. In that event and, in addition to all obligations that apply to Purchaser Data generally under the Contract, Vendor will:

(a) only Process Personal Data in accordance with applicable law and in accordance with any other written instructions given by Purchaser,

(b) to the extent that the Permitted Purpose requires Vendor to collect, extract or receive Personal Data from a Data Subject, take commercially reasonable steps to: (i) notify the Data Subject and obtain consent, or ensure there is another legal basis, to Process such Personal Data; and (ii) ensure that any such Personal Data is accurate and complete,

(c) maintain a log documenting Vendor's Processing of the Personal Data for the Permitted Purpose, including without limitation, any disclosure to, transmission to, or accessing of, the Personal Data by, Authorized Personnel.

14. Subprocessing

14.01 To the extent that Vendor engages Subprocessors, Vendor will only engage the Subprocessors included in Attachment 1 to this Data Protection Annex and will make information about such Subprocessors, including their function and location, available to Purchaser. If Vendor subsequently engages a new Subprocessor or changes the function of an existing Subprocessor ("Subprocessor Change"), Vendor will inform Purchaser at least ninety (90) days in advance, unless the Subprocessor Change is made to address an imminent or existing risk, in which case Vendor will inform Purchaser as soon as reasonably possible. If Purchaser reasonably determines that a Subprocessor Change would materially increase Purchaser's risk, Purchaser may notify Vendor and request that Vendor replace the Subprocessor with a Subprocessor reasonably acceptable to Purchaser; if Vendor does not take such action, Purchaser may terminate the Contract.

14.02 Vendor will ensure that any authorized Subprocessors are bound by data protection obligations that are substantially equivalent to, or more onerous than, the obligations set out in the Contract.

14.03 Vendor will remain responsible and liable to Purchaser for all acts and omissions of any Subprocessors in connection with the Contract and will ensure that any Subprocessors comply with all terms and conditions of the Contract.

15. Definitions

15.01 For the purposes of this Data Protection Annex:

(a) "Authorized Personnel" means only those of Vendor's employees, agents, advisors, or Subprocessors who have a need to know, or to Process, Purchaser Data for the Permitted Purpose.

(b) "Contract" means any agreement or purchase order between Purchaser and Vendor that references, attaches, or otherwise expressly incorporates this Data Protection Annex, together with the terms of this Data Protection Annex, and any other Purchaser documents referenced in, or otherwise expressly incorporated into, the agreement or purchase order.

(c) “Data Incident” means any actual or reasonably suspected unauthorized or unlawful: (i) use, modification, alteration, disclosure, transfer, interception, corruption, destruction, deletion, loss, or other Processing of, or access to, Purchaser Data, or (ii) access to, or damage, attack, corruption or loss of, any systems or devices that are used to access, host, maintain, transfer, or otherwise Process any Purchaser Data.

(d) “Data Subject” means a natural living person whose Personal Data is Processed.

(e) “Permitted Purpose” means the processing of Purchaser Data solely and exclusively to the extent necessary for Vendor to perform its obligations under the Contract.

(f) “Personal Data” means any information relating to an identified or identifiable individual. An identifiable individual is one who can be identified by reasonable means, directly or indirectly, by reference to an attribute or combination of attributes within the data or combination of the data with other available information. Attributes that can be used to identify an identifiable individual include, but are not limited to, name, identification number, location data, online identifier, metadata, and factors specific to the physiological, genetic, mental, economic, cultural, or social identity of an individual.

(g) “Process” means any operation or set of operations which is performed on Purchaser Data, or on sets of Purchaser Data, whether or not by automated means, such as accessing, capturing, collecting, extracting, recording, organizing, structuring, storing, adapting, retrieving, intercepting, using, disclosing by transmission, dissemination, hosting, transmitting, or otherwise making available, modifying, aligning or combining, restricting, erasing, deleting, or destroying.

(h) “Purchaser” means the relevant member of the World Bank Group described as the “Purchaser” in the Contract.

(i) “Purchaser Data” means any and all information, regardless of its form, that: (i) is provided by or on behalf of any member of the World Bank Group or any of its clients to Vendor or any of its representatives in connection with the Contract, (ii) is accessed by Vendor or any of its representatives via World Bank Group systems, (iii) is generated by Vendor or any of its representatives for or on behalf of any member of the World Bank Group or any of its clients in connection with the Contract, or (iv) comprises Personal Data Processed at the request, or on behalf, of the World Bank Group in connection with the Contract.

(j) “Subprocessor” means any person or entity to which Vendor (or its Subprocessor) has provided Purchaser Data or who otherwise Processes Purchaser Data on behalf of Vendor.

(k) "Third Party Data Request” means any actual or threatened request or demand by any person or entity for access to, or the production or disclosure of, any Purchaser Data, including without limitation, pursuant to any applicable law, regulation, or other form of legal process or procedure.

(l) “Vendor” means the entity or individual described as “Vendor” or “Contractor” in the Contract.

(m) “World Bank Group” means the International Bank for Reconstruction and Development, the International Finance Corporation, the International Development Association, the Multilateral Investments Guarantee Agency, and the International Centre for Settlement of Investment Disputes, each of which may be referred to as a member of the World Bank Group and collectively as members of the World Bank Group.

Annex 2 – Information Security for Contractors

1. Policy

1.1. Policy Rationale

This policy establishes basic principles and requirements for Contractors necessary for the secure use and management of the World Bank Group's ("Bank Group" or "WBG") information and information systems.

1.2. Applicability

This policy applies to all Contractors, on-site and offshore, at all locations throughout the world that are

using Bank Group systems or accessing, processing, or storing Bank Group Restricted Information, as per The World Bank Policy on Access to Information Policy (https://ppfdocuments.azureedge.net/3693.pdf), whether in electronic format or otherwise.

2. Written Information Security Program (WISP)

2.1. Contractors must implement and maintain a written information security program applicable to

the Contract, which, at a minimum, accomplishes all of the following:

Designates an Information Security Officer, which may be any employee with sufficient authority and experience to implement and maintain the written information security program;

Provides for regular training of all Contractor and Subcontractor employees on appropriate security procedures and techniques;

Provides common industry security practices and controls including AV/Malware protection;

Requires the performance of an initial and annual assessment of Contractor's security vulnerabilities;

Requires that Contractor implement appropriate safeguards to address any security vulnerabilities;

Requires the implementation and annual review of an incident response plan;

Requires the performance of an annual review of the written information security program;

Implements a process for evaluating and auditing the ability of all Subcontractors to meet the same security requirements that Contractor must meet; and

Establishes secure protocols for user authentication and user access to Bank Group information and systems.

2.2. The WISP is subject to review and approval by the WBG Office of Information Security.

3. Internal Service Providers

3.1. Internal service providers are Contractors, offsite or on Bank Group premises, that access WBG systems and information directly through the WBG network or via authorized remote connection to the WBG network. This would include Contractors working from one of Bank Group's offshore development centers (ODCs).

3.2. Information Security Training

3.2.1. All Contractor and Subcontractor employees with access to Bank Group systems or Bank Group information must complete the mandatory information security e-learning course to ensure that they fully understand their responsibilities for protecting the World Bank Group's information when provided with access privileges. Such employees must receive training on appropriate security policies and procedures on a periodic basis as decided by the Office of Information Security. Failure to comply may result in access revocation.

3.3. Information Assets and User Access

3.3.1. All Bank Group information assets (e.g. data, datasets, reports, communications, manuals, documentation for systems, procedures, and plans) are considered "Confidential", unless expressly stated otherwise by the information provider.

3.3.2. Contractors are responsible for protecting all Bank Group information and the systems which process, store and transmit such information from unauthorized disclosure and modification regardless of location. Contractors which will be using or accessing the International Finance Corporation's ("IFC's") systems, information, electronic or otherwise must abide by all relevant IFC specific policies and procedures including the IFC Policy on Disclosure of Information. Contractors must ensure that all of their staff or subcontractor staff who use or access IFC systems or information abide by such IFC policies and procedures. If there are differences between IFC policies and procedures and those in other World Bank Group policies and procedures, the IFC policies and procedures shall apply where IFC systems or information are being accessed or used.

3.3.3. Contractor and Subcontractor access rights shall be determined by the Bank Group Project Manager. Contractor and Subcontractor employees shall be granted the least amount of access to Bank Group systems and information necessary for such employees to perform their contractual functions. Any unauthorized attempt to access information that is outside the access parameters set by the Bank Group Project Manager is prohibited.

3.3.4. Contractors shall not, unless expressly authorized by the Office of Information Security (OIS) in writing, connect non-standard hardware, or personal devices to the World Bank Group's network.

3.4. User Credentials

3.4.1. User credentials are provided to Contractors by WBG to facilitate their work functions as defined

in the contract. Credentials include, but are not limited to: username, password, Multi-Factor Authentication token, and physical access badge.

3.4.2. Each Contractor is responsible for safeguarding his or her credentials, and protecting them from unauthorized use.

3.4.3. Contractors are prohibited from disclosing or sharing their credentials with others.

3.4.4. Contractors are accountable for any incident arising from improperly protected credentials. Compromised credentials must be immediately reported to the Project Manager and changed or invalidated.

3.4.5. Any unauthorized attempt to discover or obtain the credentials of another user or to access Bank Group information or systems using another person's credentials is prohibited.

3.4.6. All passwords used to access Bank Group Systems must meet the following criteria:

Passwords must be at least 8 characters in length, they must be sufficiently complex that they cannot be easily guessed, and they must use both alphanumeric and special characters;

Passwords must be changed every 90 days;

Users shall not repeat any of his or her last 5 passwords;

Upon receiving access credentials, users shall immediately change the password to a unique value known only to the user;

Users shall not rely on default passwords;

Contractor shall prohibit users from sharing passwords with anyone; and

Contractor shall prohibit users from recording passwords on paper or in a document.

3.5. Information Systems Use

3.5.1. All Bank Group information systems (i.e. email, internet, telephones, fax, etc.) are the property of the Bank Group and are primarily for Bank Group business use. Contractors may use them for incidental personal purposes, as defined by the Acceptable Use Policy, and must never use them to knowingly access, store, or distribute pornographic or otherwise offensive or illegal material.

Contractors may not use Bank Group systems to knowingly compromise other Bank Group systems, networks or safeguards.

3.5.2. Contractor personnel shall not install, modify, or uninstall software on any device that is used to access the Bank Group systems or Bank Group information without the explicit authorization of the Project Manager.

3.5.3. Contractor's computers, laptops, smart phones, and other devices or portable media assigned by the Bank Group and/or containing Bank Group information must be secured by their users from theft and unauthorized use and may not be left unattended in a public space, including in a personal vehicle.

3.5.4. Contractors may not leave unattended in a non-public space any device containing Bank Group information unless a password-enabled locking mechanism is engaged.

3.5.5. To ensure information security and integrity, Contractors must always completely log out from all applications, leave desktop computers in a locked state, turn off peripheral devices, and lock cabinets and other information storage containers when left unattended.

3.5.6. All systems and software packages must be fully tested for system compatibility and for the presence of malicious code and covert channels by the Office of Information Security (OIS) before installation and use.

3.5.7. Contractors may not remove equipment from Bank Group facilities without explicit authorization

from the Project Manager.

3.5.8. Contractors must always backup critical electronic files to an appropriate network drive as authorized by the Project Manager.

3.5.9. Contractors must ensure that all information is removed from devices or storage containers that are moved off-site and are no longer under their direct control. If in electronic format, information must be overwritten, not just deleted. Contractors must provide the Bank Group with a documented process for information removal/destruction and written verification of specific implementation of this process as it relates to the subject contract.

3.6. Encryption

3.6.1. Contractors shall use encryption to protect all Bank Group information from inadvertent disclosure when such information is sent over the Internet or other open, non-Bank Group networks. Such encryption must meet industry standards.

3.6.2. Contractors shall use encryption whenever possible when transmitting Bank Group information within the Bank Group network.

3.6.3. Contractors are prohibited from removing any information from the Bank Group network unless strictly necessary to perform a function under its contract and authorized by the Project Manager. Any information that is not stored on the Bank Group network must be encrypted and must be stored on a network that meets the standards set out in Section 4: External Service Provider Requirements.

3.7. Malicious Code

3.7.1. Contractors must use up-to-date malicious code protection (including anti-virus) software for all

systems and devices that are used to access Bank Group systems or Bank Group information.

3.7.2. Contractors are prohibited from introducing malicious code into Bank Group systems, software,

or devices.

3.7.3. Contractors are prohibited from attempting to bypass Bank Group malicious code protection

software or other system safeguards (e.g. when downloading or transferring information).

3.7.4. Contractors must always use installed Bank Group malicious code protection software and other system safeguards. Contractors must scan all files and software before introducing them to Bank Group systems.

3.8. Incident Reporting

3.8.1. All information security incidents (e.g. malicious code, worms, viruses, unauthorized or inappropriate email/internet use) must be immediately reported to the Global Support Center and Project Manager upon discovery. In no event shall Contractor take longer than 24 hours to report a security incident.

3.8.2. Loss of Bank Group assigned desktop, portable, or mobile computing devices by any means (e.g. theft, loss, breakage) must be reported to the Global Support Center and Project Manager as soon as discovered.

3.9. Telecommunications Security

3.9.1. Contractors are responsible for being aware of current and potential telecommunications (e.g. telephones, voice mail, mobile phones, conference calls, instant messaging, and facsimile machines) security risks in their given environment, and must always consider information sensitivity and transmission security issues when selecting a communications medium.

3.10. Remote Access

3.10.1. Remote access refers to Contractors using telecommunications/remote access to conduct their authorized activities from a location other than WBG networks.

3.10.2. All Bank Group-owned desktop, portable or mobile computing devices must employ access control and user authentication mechanisms that have been approved by the Project Manager for access to the Bank Group's network.

3.10.3. For remote access using non-Bank Group owned computing devices, access will be controlled through an access account, the granting of which will be coordinated by the Project Manager. All

non-Bank Group owned computing devices that are granted access to Bank Group systems must comply with all security requirements set out in this policy.

3.10.4. Authentication and information transmitted during a remote access session must be encrypted end-to-end and the session must be terminated when work is completed or when the remote access device will be left unattended.

4. External Service Provider Requirements

4.1. An External Service Provider (ESP) is a Contractor that hosts, stores, and/or processes Bank Group information and/or applications off Bank Group premises.

4.2. Pre-Engagement Requirements

4.2.1. The ESP must provide an overview of their information security management system including information security policies to the Project Manager for Bank Group review prior to the engagement.

4.2.2. The ESP must provide the Bank Group with an audit report of their information security management system conducted by a certified auditor when requested by the Bank Group.

4.2.3. A Service Level Agreement must be part of the contract between the ESP and the Bank Group.

4.2.4. The ESP must assign a single point of contact for the resolution of information security related issues and must notify the Sponsoring Business Unit and the Bank Group's Office of Information Security (OIS) in writing.

4.3. Personnel Requirements

4.3.1. All Contractor and Subcontractor personnel with access to Bank Group information, regardless of the location where such information is maintained, must complete the information security training requirements or equivalent identified above.

4.3.2. Any change in operational or security administration personnel assigned to Bank Group information systems must be communicated to the Sponsoring Business Unit and the OIS in writing.

4.3.3. The ESP must disclose who among its personnel and/or personnel of other entities will have access to the environment hosting the Bank Group's information or systems.

4.3.4. No Bank Group staff other than those authorized by the Sponsoring Business Unit should be given access to Bank Group information and systems.

4.4. Subcontractor Requirements

4.4.1. Before providing a subcontractor with access to Bank Group information, the ESP must ensure that all subcontractors and/or third parties engaged in the fulfillment of its contract with the Bank Group are aware of and agree in writing to adhere to all provisions contained in this Bank Group policy.

4.4.2. ESP must maintain a network monitoring capability along with appropriate user authentication

procedures that will allow it to identify when a subcontractor has accessed the ESP's systems and what information the subcontractor accessed.

4.4.3. ESP must ensure that the subcontractor maintains an environment with equivalent or higher controls, policies and procedures than those applicable to ESP.

4.5. ESP Communications and Operations Security

4.5.1. On notification from the Sponsoring Business Unit, the ESP must be able to immediately disable all or part of the functionality of the application or systems should a security issue be identified.

4.5.2. The ESP must employ up-to-date malicious code protection software or systems to ensure the confidentiality, integrity, and availability of Bank Group information and information systems.

4.5.3. The ESP's System Administrators must maintain complete, accurate, and up-to-date information regarding the configuration of Bank Group hosted systems. This information must be made available to designated Bank Group personnel upon request.

4.5.4. The ESP must have a patch management process that includes the testing of patches before installation on Bank Group systems and on any ESP systems that host Bank Group information. Patch notifications must be communicated to the Sponsoring Business Unit.

4.5.5. The network hosting Bank Group applications must be logically isolated and/or segmented, separating the Bank Group systems network from other networks or customers that the ESP may have.

4.5.6. Host and network intrusion detection must be employed by the ESP where Bank Group systems

are located. The ESP must also use data loss prevention software on any systems that host or have access to Bank Group information.

4.5.7. The ESP must subscribe to vulnerability intelligence services or to Information Security Advisories and other relevant sources providing current information about system vulnerabilities.

4.5.8. All changes to system configurations, services enabled, and permitted connectivity must be logged and the logs must be retained for a Bank Group prescribed period.

4.5.9. All system and user activities, including the ones which might be an indication of unauthorized usage or an attempt to compromise security measures must be logged for systems that process or store Bank Group information.

4.5.10. ESP must block access to any account following 5 failed log-in attempts. Access may not be restored until ESP security personnel have confirmed the identity of the user and the user's access privileges.

4.5.11. For all Bank Group applications and systems running Bank Group applications, log files must be

protected to ensure confidentiality and integrity.

4.5.12. The Bank Group reserves the right to periodically audit the ESP to ensure compliance with the

Bank Group's security policy and standards.

4.5.13. The ESP must perform daily backups of Bank Group information and systems, and safeguard all

backup media.

4.5.14. The ESP must be able to adhere to Bank Group's data retention requirements.

4.5.15. The ESP must perform periodic tests on its control environment and provide 3rd party

attestations to the Bank Group upon request.

5. Procedures

Access to procedures are available on a need-to-know basis. For access, contact the OIS.