SBS Saas Product Description Risk Assessment

SBS SaaS Product Description_Risk Assessment_(eng)_v07042025

Summary

1. Introduction

This product description for the “Risk Assessment” SBS Offering forms part of the Agreement between SBS and Customer. All capitalized terms not defined in this Document will have the meaning given to them in other parts of the Agreement.

Risk Assessment is a SaaS risk analysis solution. Designed for financial institutions, it can be integrated into their systems via API or used directly through the web application. It enables financial institutions to instantly obtain a comprehensive risk analysis of a company. Risk Assessment analyses financial, banking, managerial, and environmental data of a company. The solution also offers Document classification, data extraction, and Document fraud detection.

Risk Assessment supports a wide range of Documents, such as Bank statements, Financial statements, legal statutes, bank identity statements, and anti-money laundering declarations.

The different modules available are as follows:

- **Identity and Financial Data**: module that connects to external databases to retrieve company data and Financial Statements.
- **Financial X-Ray**: instant credit-risk scoring module based on financial, macroeconomic, and behavioural data assessing the probability of default.
- **Bank X-Ray**: decision support module which aggregates and analyses a company’s banking transactions to monitor the evolution of a company’s cash flow, detect signs of economic distress and detect suspicious behaviour.
- **Doc X-Ray**: module that on one hand estimates the authenticity and correctness of PDF Documents, and on the other hand extracts and classifies information from the analysed Documents.
- **Manager X-Ray**: risk analysis module that evaluates the company’s history, as well as that of its managers and Ultimate Beneficial Owners (UBOs), using public data sources to detect suspicious behaviour related to the company or its executives.

2. Usage of SaaS Risk Assessment

2.1. Process for creating a Customer Area

When the Account Manager creates the account, the Customer receives an automated email containing an activation link to access their secure Customer Area. This space is exclusively reserved for Authorized Users and provides access to the Services related to the Risk Assessment platform.

Authorized Users can modify their login credentials and update their contact information once logged into their account via their profile. They can also create a new password using a secure two-factor authentication process.

The Customer is responsible for the use and storage of their access codes and will personally deal with the consequences arising from their disclosure or misuse. The Customer must consequently, and in their own interest, take all necessary measures to ensure their security and strictest confidentiality. The Customer shall be solely liable for any fraudulent or improper use of the Risk Assessment platform due to voluntary or involuntary disclosure of the access codes to anyone.

2.2. Authorized Users' roles and access management

Risk Assessment provides advanced role and access management, ensuring that roles are assigned to Authorized Users based on their responsibilities.

Once the Account Manager has created the Customer's organization, an Owner is assigned to it. The Owner is the first Authorized User linked to the workspace, has full access, and can manage the roles of other members. The Owner has the right to add or remove members from the workspace. Additionally, the Owner can view all files created on the platform, both their own and those of other members.

Member permissions are more restricted. Members can only view the Cases they have created and are not authorized to add or remove other members from the workspace.

If an Authorized User's role needs to be changed, there are two options:

- The Account Manager can make the modification.
- The workspace Owner also can modify member roles.

2.3. Service operation process

2.3.1. Filing of Documents by the Customer on the platform

To create a risk analysis file in Risk Assessment, the Authorized User must navigate to the "Case" tab from the main menu and follow the steps to "Create Case." By entering the company's identification number (SIREN, CIF, CF, CREFO, KvK, depending on the country), the platform will automatically retrieve information from external and internal data sources.

After this initial data collection, the Authorized User can upload additional Documents to enable the X-Ray tools to generate in-depth analyses.

Risk Assessment supports several types of Documents, with the most used being:

- Bank Statements.
- Financial Statements.
- Legal statutes.

- Bank identity statements.
- Anti-money laundering declarations.

To ensure efficient data extraction, files must be in native PDF format. In the case of scanned Documents, OCR (Optical Character Recognition) technology allows the Documents to be analyzed and relevant information to be extracted. However, a scanned or low-quality PDF, which is an image of a printed Document, will not allow for reliable data extraction. Document fraud detection will not be possible with this type of file.

Additionally, Authorized Users can add extra Documents to a Case even after its creation via the “Documents” tabs. Documents can be uploaded using the "Upload Documents" button.

A specific Case can be found by entering its name in the search bar within the "Documents" tab.

2.3.2. Access by SBS to Customer Area

For several reasons, including technical maintenance, SBS may, if necessary, access the Customer Area to ensure the proper functioning of the Services. This access is regulated, limited to a small number of authorized operators, and guarantees data confidentiality.

2.3.3. Storage of data and processing results

To comply with the statutory and regulatory obligations of the Customer, SBS is offering to store the data entered or uploaded by the Customer for a period of two (2) years from the moment the Services process the data.

The storage of data by SBS does not discharge the Customer of its obligations to store data towards its own customers, and they undertake to take all useful measures to store the data and indicators obtained using the Services.

It is the Customer’s responsibility to regularly extract, save and print the data entered and the information produced in the Customer’s space, and to keep a copy of the Documents from which they extract the data to ensure archiving and to allow an audit, if required, of their activities by the relevant administrative authorities.

3. Detailed Description

3.1. Authorized User’s interface

Authorized Users of the Risk Assessment platform have access to an intuitive interface that makes it easy to manage Cases. Upon logging into the platform, the dashboard provides an overview of both ongoing and completed Cases. The interface includes several tabs accessible through the main menu, where Authorized Users can initiate new Cases, navigate through existing ones, access personal information, and manage organizational settings.

In the Cases tab, Authorized Users can view and manage Cases based on their assigned roles and permissions. This section also allows for an in-depth review of the analyses and results of a Case, as Authorized Users can simply click on a Case to obtain more information.

A Case contains one or more analyses related to a company. Cases are used to analyse and assess a company's or an individual’s financial information using X-Ray tools, which assign scores ranging from A to E and generate detailed visual reports. Authorized Users can also add additional Documents or files to a Case at any time to refine the analysis, even after the Case has been created.

The analysis follows several structured steps that enable financial institutions to streamline their risk assessment process. The platform is designed to collect and process data in multiple stages: retrieving a company’s legal and financial information,

conducting an in-depth analysis through X-Ray modules, and generating decision-support reports. Each evaluation is stored in a Case, making it easier to monitor the companies being analysed over time.

A personal space is also available, allowing Authorized Users to modify their information and update their password.

Finally, the account Owner can manage Authorized Users and customize organizational settings. For instance, the account Owner can add or remove members and adjust company-related information to optimize team management and analysis processes.

3.2. Risk analysis tools

Risk Assessment is based on a company data retrieval module and four analysis modules, enabling financial institutions to obtain a comprehensive and instant view of a company through a fully digitalized, fast, and secure process.

3.2.1. Identity and Financial Data

The identity and financial data retrieval component allows for the collection of the following information:

Company Data:

Information	Description	Manual Entry [1]
SIREN	Unique identification number assigned to each company in France. It is used to legally identify a company with the authorities.	Not editable
NACE	This code describes the company's activity according to the European nomenclature.	Editable
Creation date	Official date of company creation. It allows determining the organization's age.	Editable
Time in business	Duration of activity since the company was created.	Calculated
Location	Refers to the city where the company is registered.	Editable
Zip code	The postal code identifies the geographic area where the company is located.	Not editable
Employees	Estimate of the number of employees in the company.	Editable

[1] *Note: The Authorized User can manually enter certain data to modify or complete automatically collected information.*

Asset Components and Liquidity Indicators:

Assets	Description	Manual Entry [1]
Months passed	Number of months since the fiscal year-end of the most recent Financial Statement.	Editable
Opening balance	Bank balance amount at the beginning of the period.	Not editable
Closing balance	Bank balance amount at the end of the period.	Not editable
Balance level	Lowest bank balance recorded during the period.	Not editable
Average monthly balance	The average balance maintained in bank accounts over a month.	Not editable
Inventory	Total amount of physical stocks the company holds.	Editable
Accounts receivables net	Total amount of receivables due from Customers, minus amounts unlikely to be paid.	Editable
Cash available	Funds available in the company's bank accounts.	Editable

Total fixed assets	Assets intended to be held long-term (more than 1 year) by a company (e.g., land, buildings, and equipment).	Editable
Total assets	Total value of assets held by the company.	Editable
Current assets	Short-term assets (less than 1 year) used for the company's regular operations.	Editable
Operating working capital requirement	Indicator that evaluates the company's short-term liquidity. Short-term assets minus liabilities needed for daily operations.	Calculated

[1] *Note: The Authorized User can manually enter certain data to modify or complete automatically collected information.*

Liability Components and Financial Structure:

Liabilities	Description	Manual Entry [1]
Equity	Total company's asset ownership after deducting liabilities.	Editable
Capital	The money permanently provided to the company by its owners or partners, either at creation or during company's growth.	Editable
Bank debt	Total amount of loans owed to banks or financial institutions.	Editable
Bonds debt	Total amount of debt in the form of bonds, issued as debt securities.	Editable
Other financial debt	Groups other types of financial debt not classified as bank debt or bonds debt.	Editable
Short-term debt	Total amount of short-term debt, due within one year.	Editable
Loans received	Amount received by the company as loans.	Not editable
Accounts payables	Purchases made by the company from suppliers that have not yet been paid.	Editable
Current liabilities	All short-term financial obligations of the company due in one year.	Editable
Total liabilities	Total sum of all liabilities, including debts, other financial obligations and non-financial obligations.	Editable
Total financial debt	Total amount of debt contracted by the company with financial institutions and other creditors.	Editable

[1] *Note: The Authorized User can manually enter certain data to modify or complete automatically collected information.*

Profit & Loss:

Title	Description	Manual Entry [1]
Turnover	Total revenue generated by the company through its main activity.	Editable
Cash generated	Available cash after revenue collection and expense payment.	Not editable
Amortization & Depreciation	Allocation of an asset's acquisition cost over its usage period and loss of value.	Editable
Operating income	Revenues minus operating expenses: Profit from core business activities.	Editable
Interest expense	Interest paid on debts and other financing costs.	Editable

Income tax	Amount of taxes paid by the company.	Editable
Positive or negative net income	Profit or loss after deducting all expenses and taxes from revenue.	Editable
Fiscal year duration	The duration of the company's fiscal year.	Editable
Legal procedure	Indicates whether there is an ongoing legal procedure.	Editable
EBITDA	The company's operating profitability; Earnings before interest, taxes, depreciation, and amortization.	Calculated

[1] *Note: The Authorized User can manually enter certain data to modify or complete automatically collected information.*

3.2.2. Financial X-Ray

Financial X-Ray is an instant credit risk scoring module based on financial, macroeconomic, and behavioural data to assess the probability of default. This model is designed to predict the likelihood of a company defaulting and failing to meet its financial obligations within the next 12 months. Financial X-Ray evaluates this potential default probability and converts it into a rating ranging from A to E (from low to high probability of default). To achieve this, the module relies on 50 key indicators, including 10 primary ones that directly influence the rating, allowing Authorized Users to understand how the score was assigned.

Developed in France, Italy, Spain, and the Netherlands, this model is based on four different Machine Learning models, each with its own thresholds.

To generate a Financial X-Ray score, the Authorized User must provide the company's identification number when creating a Case. This allows the module to collect data from both external and internal sources. If financial Documents have not been uploaded or are unavailable, the Authorized User can also upload the company's most recent Financial Statements.

To automatically estimate the default rate, Financial X-Ray takes multiple data points into account for its analysis. It gathers the latest available information from external databases as well as from the uploaded Financial Statements.

Additionally, if multiple Financial Statements are uploaded, the technology will automatically identify the most recent Document to extract the necessary data for generating the Financial X-Ray report.

Using machine learning, the module can determine the positive or negative impact of a company's industry sector or operational lifespan on the score. Furthermore, the company's management history analysis, through Manager X-Ray, can also be integrated into the risk assessment, influencing the final score positively or negatively.

Once the analysis is completed, Financial X-Ray displays a score and a default probability directly on the platform. It also generates a detailed visual report, highlighting the impact of different indicators on the final rating.

Finally, it is possible to update the Financial X-Ray report by adding new Financial Statements or modifying company data from the "Business data" tab within the Case. This feature is useful for testing different scenarios based on financial projections or interim Financial Statements.

3.2.3. Bank X-Ray

Bank X-Ray is a decision-support module that aggregates and analyses a company's banking transactions to monitor cash flow trends, detect signs of financial distress, and identify suspicious behaviours.

Bank X-Ray can be used for three main purposes:

- Risk Analysis: providing a real-time overview of a company's cash flow management and automatically identifying potential signs of financial distress. This complements previous analyses by adding relevant insights.
- Fraud Detection: identifying inconsistencies that may indicate fraudulent behaviour or attempts at financial manipulation based on banking transaction data.
- Portfolio monitoring: tracking the financial evolution of Customer's customers over time by regularly updating their Bank X-Ray report to anticipate potential risks.

A Bank X-Ray report is based on Customer's customers' transactions extracted from PDF Bank Statements, as well as on Open Banking transactions that the Customer's customer has collected and transferred to the platform.

Once Bank Statements are obtained:

1. The Authorized User creates a Case or accesses an existing one:
   - If the Bank Statements belong to a company that does not yet have a Case on the platform, a new Case must first be created.
   - If the Bank Statements belong to a company with an existing Case, it can be found in the Cases tab using the search bar.
2. Upload the Bank Statements: Within the company's Case, navigate to the Documents tab and upload the files.

After uploading, the Doc X-Ray module will automatically analyse the Bank Statements to extract the necessary data. This process typically takes a few minutes. Data integrity checks are performed to ensure the good extraction of values.

Bank X-Ray is a module that aggregates, categorizes, and analyses banking data to provide a real-time financial health report for the Customer's customers. Each time a new Bank Statement is uploaded to the platform, a new Bank X-Ray report is generated.

It is important to note that if the data integrity level, which refers to the quality of extracted data, is below 70% (default threshold, adjustable upon request), no rating will be assigned to the Bank X-Ray report.

The data integrity level represents the percentage of transactions successfully extracted from the Bank Statements. This percentage serves as a quality indicator for the Bank X-Ray report, calculated across all analysed Bank Statements and providing an overall evaluation.

Once the extraction is successfully completed, a new Bank X-Ray report is generated and will be available in the corresponding tab within the company's Case.

All this information is gathered in a visual Bank X-Ray report providing extensive details on:

- **The Bank X-Ray Score**: gives an overall assessment of the company's financial health using a letter rating system ranging from A to E (positive to negative).
- **The "Balance" section**: provides a visual overview of how the company manages its cash flow over a predefined period. This chart includes cash inflows and outflows as well as the balance evolution. Additionally, below the chart, a complementary table provides information on credits and debits, the company's financial health, and the stability of the bank account. For optimal analysis, it is recommended to upload at least six months of banking transactions to identify trends or seasonality in the activity of the customer.
- **Counterparties**: a mapping of regular financial partners classified based on their frequency of appearance in transactions. Intercompany transfers are also highlighted.
- **A company's payment**: behavior regarding wages, social security, taxes and financial suppliers through a series of charts. In addition to the graphs, additional information is also present on the monthly averages paid and the maximum deviation in number of days compared to the normal payment frequency.
- **Alerts**: with a section that highlights transactions containing specific predefined keywords (such as late payment fees, legal proceedings, fund withdrawals, inter-company transfers, among others) and customizable. This feature allows for the quick identification of transactions requiring further analysis, making decision-making easier
- **Detailed Transactions**: Groups all transactions extracted from Bank Statements, sorted chronologically. Each transaction includes bank account details, daily balances, and the type of movement (credit or debit). This section is used to gain more insights into a specific transaction or analyze a particular counterparty. Filters are available to sort transactions by type, category, name, or amount.

The first section of the report presents an overall score, rated from A to E (from positive to negative), obtained by comparing several financial and behavioral indicators with companies in the same sector. Each indicator is evaluated individually and then combined to calculate the overall score. This score is based on the aggregation of nine relevant financial and behavioral indicators, ranked in descending order of importance in the score calculation. These indicators are as follows:

Indicator	Description	Scoring method
Alert Frequency	Ratio of transactions with alerts to total transactions.	Benchmark on Cases from companies belonging to the same sector and country.
Alert-related amount	Significant amounts on transactions with alerts.	Benchmark on Cases from companies belonging to the same sector and country.
Overdraft	Number of days with negative balance.	Benchmark on Cases from companies belonging to the same sector and country.
Social security	Regularity of monthly social security payments.	Hardcoded rule.
Tax payment	Regularity of tax payments.	Hardcoded rule.
Payroll Management	Regularity of monthly salary payments.	Hardcoded rule.
Debt stress	Ratio of existing debt to cash generated.	Benchmark on Cases from companies belonging to the same sector and country.
Whole-number amounts	Ratio of transactions with whole-number amounts to total transactions.	Benchmark on Cases from companies belonging to the same sector and country.
Balance trend	Important deviation between opening balance and ending balance.	Benchmark on Cases from companies belonging to the same sector and country.

The scoring rule based on a comparison with Cases of companies in the same sector and country is determined as follows:

- A: The indicator is better than 90% of benchmark.
- B: The indicator is better than 70% and under 90% of benchmark.
- C: The indicator is better than 50% and under 70% of benchmark.
- D: The indicator is better than 20% and under 50% of benchmark.
- E: The indicator is worse than 20% of benchmark.

The business rule-based scoring is determined as follows:

- A: Payments are made regularly.
- C: Payments are delayed in less than 40% of Cases.
- E: Payments are delayed in more than 40% of Cases, and no payments have been made for 3 months.

The overall Bank X-Ray score is based on:

- The score assigned to each indicator (C, D, and E scores will generate alerts),
- The weight of each indicator on the scoring model.

3.2.4. Doc X-Ray

Doc X-Ray is a module designed to verify the authenticity and accuracy of Documents (in PDF format) while also extracting information from Financial Statements and Bank Statements. With its machine learning algorithm, the module automates Document management and identifies potential fraud in analyzed Documents.

Authorized Users can add Documents in two ways: manually uploading them directly to the platform or via the API when creating or updating a Case. Once files are submitted, Doc X-Ray automatically analyzes their content. For native PDFs, the data is read directly from the file and mapped using predefined templates. For non-native PDFs (e.g., scanned Documents), Doc X-Ray uses Optical Character Recognition (OCR) technology to extract the information; however, extraction may be less reliable on this type of Document. In a native PDF, text is separated from images and metadata. Each time a PDF Document is uploaded, Doc X-Ray analyzes it and automatically identifies its type. It can recognize various Documents, including Financial Statements, Bank Statements, legal Documents, identity Documents, and business Documents. The content of these Documents is extracted in a structured, machine-readable format (JSON). Once classified, these Documents are automatically grouped by category in the Documents tab.

For Financial Statements and Bank Statements, Doc X-Ray searches for start and end dates to assign a period to the Document. For Bank Statements, it can recognize monthly, quarterly, semi-annual, or annual periods.

Doc X-Ray is trained on tens of thousands of Documents analyzed in six different languages. Authorized Users can manually adjust alerts to enhance analysis and adapt fraud detection to their specific needs. The tool continuously learns to improve analysis accuracy and enhance automatic Document classification.

The extraction status is displayed in the Analysis Details section of the Doc X-Ray tab:

- In Progress: The Document is being analysed.
- Analysed: The data has been successfully extracted, and a new Doc X-Ray report has been generated.
- Failed: The data extraction was unsuccessful, and no new Doc X-Ray report will be generated.
- Blocked: Corrupted PDFs or files containing viruses are marked as blocked, allowing the Authorized User to delete them or upload new ones.

Doc X-Ray includes a central tool, Doc Viewer, which allows Customers to view their customers' Documents on the Risk Assessment platform. It consists of three tabs for each Document:

- "Doc view", which displays the Document and any associated alerts.
- "Docs Comparison", which allows Authorized Users to compare the first and last detected versions of a modified Document.
- "Docs Info", which provides an overview of key details related to how the Document was generated.

Using OCR, Doc X-Ray can extract the type and period of each Document and categorize them into groups within the Documents tab. Additionally, it analyzes metadata and text within PDFs to ensure their authenticity. If modifications or manipulations are detected, alerts will appear in Doc Viewer, explaining why a Document is considered suspicious or fraudulent. Based on the number and severity of alerts triggered for each Document, an overall rating is assigned, ranging from A to E (from positive to negative).

Doc X-Ray helps centralize and organize Document management for end customers. Customer benefits from an overview of their customers' Documentation, which is automatically analyzed and classified.

The Doc X-Ray module performs 11 verification checks on uploaded Documents to detect potential fraud attempts. Whenever a suspicious element is identified, an alert is triggered. These alerts fall into two main categories:

1. Document Content Verification: detects modifications made to the text or images in the Document.
2. Document Structure Verification: identifies fake or altered Documents created using specific editing tools.

Generated alerts are classified by severity level:

- Fraudulent: This alert level is automatically displayed when both the "deliberately modified Document" and "different creation and modification dates" alerts appear on the same Document.
- Moderate Risk: This alert level is displayed if either the "deliberately modified Document" OR "different creation and modification dates" alerts appear. The alert level is also considered moderate if one of the following checks generates a moderate risk:

  - Edited with suspicious software.
  - Unreliable creation tool.
  - Inconsistent font.
  - Overlapping text.
  - Digital fingerprint.
- Low Risk: This flag is displayed if no "fraudulent" or "moderate risk" alerts appear in the Document.

For example, a "Modified Text" alert is considered fraudulent, while an "Inconsistent Font" alert is classified as moderate.

Alert Name	Definition	Alert Category	Severity
Edited text	Certain parts of the text have been altered and differ from the original version. These modifications are highlighted in the Document using red boxes.	Content	Fraudulent
Inconsistent font	Consecutive letters or numbers have fonts and sizes that differ from the rest of the Document. These inconsistencies are highlighted in the Document using yellow boxes. This alert may indicate either an attempt at fraud or an error in the Document.	Content	Moderate
Overlaid & overlapped text	A block (with or without text) covering an existing text element. In this Case, the original text remains visible in the PDF metadata. These modifications are highlighted in the Document using yellow boxes.	Content	Moderate
Purposefully altered Document	Multiple versions of the same Document have been detected. Clicking on this alert redirects to the "Document Comparison" tab to compare the original version of the Document with the latest detected version.	Document structure	Fraudulent
Encrypted Document	Document protected from modifications. Encrypted Documents cannot be analyzed by our OCR technology.	Document structure	Moderate
Questionable creator tool	The Document has been created using a tool allowing modifications on the Document, such as Word or Adobe InDesign. The “Creator” can be found in the Doc Info tab.	Document structure	Moderate
Edited by a suspicious software	The Document was edited using software that allows modifications, such as Adobe Acrobat.	Document structure	Moderate
Different creation and modification dates	Each Document has a digital signature that includes the creation date and the last modification date. If these dates do not match, it indicates that the Document was modified after its generation.	Document structure	Moderate
Different generation and upload times	This check calculates the time between the Document's creation and its upload to Risk Assessment. A very short time gap may indicate potential modifications.	Document structure	Moderate

Fingerprint	To prevent fraudsters from bypassing our controls, we compare the Document with a set of similar Documents to detect unusual elements. This is only available for specific Documents.	Document structure	Moderate
Document integrity	Each PDF source code includes a summary table indicating the PDF structure. If the structure of the uploaded PDF does not match the summary table, the Document has been modified.	Document structure	Moderate

The overall Doc X-Ray score is calculated at the Case level. This score is based on the severity and number of alerts detected across all Documents linked to the Case. It is then compared to the scores of other companies in the same sector and geographic area and converted into a rating ranging from A to E (from positive to negative).

Finally, if Doc X-Ray is unable to correctly identify the type or period of a Document, or if there is an error in automatic categorization, these details can be manually adjusted. To do so, the Authorized User must select the Document to modify, choose the appropriate Document type, adjust the period if necessary, and save the changes to update the information. If the IBAN has not been correctly extracted or is missing, it can also be added by clicking the "Edit" button in the "Bank Data Extraction" section and entering the IBAN displayed on the Document.

3.2.5. Manager X-Ray

Manager X-Ray is a risk analysis module that evaluates the company's history, its background, as well as that of its executives and Ultimate Beneficial Owners (UBOs), enabling the detection of suspicious behaviors related to the company or its leaders.

Using various public data sources, Manager X-Ray triggers alerts related to past events associated with the company and its leader, then converts them into a rating ranging from A to E (from low to high risk). To ensure the relevance of alerts, a confidence percentage is assigned to each manager's identity, which influences the overall Manager X-Ray score. This evaluation is presented in a report that details the different identified alerts and their impact on the overall Manager X-Ray score.

The Manager X-Ray report consists of several sections:

- The overall Manager X-Ray score: based on the different alerts identified in the report.
- A company overview: provides information on recent changes within the company and highlights general alerts related to the behavior of the company and its executives.
- A list of all managers and Ultimate Beneficial Owners (UBOs) associated with the company, including details on:
  - Their identity.
  - Their status within the company (active or inactive).
  - Their entry date into the company.
  - The number of other companies they are linked to.
  - Any potential alerts related to these companies.

To provide a complete overview of executives, Manager X-Ray extracts personal data from public databases, including their date and place of birth. The SIREN and personal data of managers allow for assigning a confidence level to each executive and/or Ultimate Beneficial Owner (UBOs) associated with the company.

The confidence level in identity can reach:

- 100%: when Manager X-Ray can identify the manager using the SIREN, date, and place of birth.
- 50%: when Manager X-Ray can identify the manager using only the date and place of birth.

It is important to note that Manager X-Ray alerts are only relevant if the confidence level in the leader’s identity is high. A confidence level below 40% will invalidate the alerts generated by Manager X-Ray.

Based on public data, Manager X-Ray generates alerts to flag specific events related to a company, its executives, and its Ultimate Beneficial Owners (UBOs). These alerts are classified according to their severity using a color code:

- Yellow indicates a moderate alert level.
- Red indicates a high alert level.

The Manager X-Ray tool can identify the following alerts:

Alert Type	Target	Yellow	Red
Number of account publications	Company	3 Financial Statement publications over a 2-year period, regardless of when they occurred.	More than 3 publications of accounts within a period of 2 years, no matter how long ago this happened OR 3 publications of accounts within the last 3 years AND at least 2 company moves in the last 3 years.
Number of address changes	Company	1 move in the last 3 years.	The company has moved once in the last 3 years AND has 3 publications of accounts within a period of 2 years, no matter how long ago this happened.
Number of legal procedures	Company		The company is under procedure or closed
Number of manager's replacements	Managers and UBOs	More than 50% of administrators are replaced in less than 18 months.	
Number of alerts on companies related to a manager	Managers and UBOs	The manager has been involved in less than 3 legal procedures that occurred in the last 5 years AND the confidence level in the manager's identity is between 40% and 60% AND the manager was actively related to the company at that time OR The manager has been involved in more than 3 legal procedures that occurred more than 5 years ago AND the confidence level in manager's identity is between 40% and 60% AND the manager was no longer active in the company for 1 year.	The manager has been involved in less than 3 legal procedures that occurred in the last 5 years AND the confidence level in manager's identity is superior to 60% AND the manager was actively related to the company at that time OR The manager has been involved in more than 3 legal procedures that occurred more than 5 years ago AND the confidence level in manager's identity is superior to 60% AND the manager was actively related to the company at that time.
Hidden manager[2]	Managers and UBOs	If the confidence level in the manager's identity is between 60% and 100% and the manager can be found on BODACC.	If the confidence level on the manager's identity is equal to 100% and the manager can be found on BODACC.

Number of major alerts per manager	Managers and UBOs		The manager is legally banned from running a company or creating one.

[2] *This alert appears when we suspect that an executive has requested to be removed from databases under the right to be forgotten legislation, but we have found through the Official Bulletin of Civil and Commercial Announcements (BODACC) that this person is still associated with the company.*

Finally, an overall score is assigned to the Manager X-Ray report, ranging from A to E (positive to negative), reflecting the number and severity of alerts raised about a company and its managers:

- A: No alerts.
- B: Up to one yellow alert on leader and UBOs.
- C: Up to two yellow alerts on executives and UBOs.
- D: Up to five yellow alerts, either on the company, its managers, or UBOs, or one red alert concerning a company linked to a manager.
- E: A red alert is triggered when one of the following elements is detected: three account publications in the past two years, or at least one manager with a major alert, or the presence of a hidden manager.

3.3. Access to the Service

Access to the Service is provided as follows:

- Web Application: the Customer can submit Cases using the company's registration code. They can also upload the necessary Documents and access the selected modules for analysis.
- Application Programming Interface (API): the Customer can submit Cases via the secure API by uploading Documents and sending the company's registration code. They will access the chosen Service scores through a secure API connection. This information is shared in JSON format.

4. Glossary

“Case” refers to an analysis of an organization's or an individual's financial information using X-Ray tools that generate scores ranging from A to E and provide visual reports. A Case enable Customer to evaluate risk and make informed lending decisions.

“Document” refers to a file uploaded by Customer in a Case, such as a Financial Statement, Bank Statement, or ID card. The Doc X-Ray system processes this file to detect fraud and extract relevant data.

“PSD2 Connection” refers to a secure bank connection under the European Union's Payment Services Directive 2 (PSD2). A PSD2 Connection provides a secure way to connect directly to bank accounts, allowing access to bank transaction data.

“Bank Statement” refers to an official summary of financial transactions (debit and credit) occurring within a given period (monthly, quarterly, or yearly) for each bank account held by an individual or an organization with a financial institution. PDF Bank Statements are subject to the Doc X-Ray limitation. A PDF Bank Statement encompassing N months within a single Document shall be regarded as equivalent to N individual Documents.

“Financial Statement” refers to a formal record of the financial activities and position of an individual or organization.

“Customer Area” refers to the Authorized User interface on the Risk Assessment platform. To access it, log in to the platform, go to your profile, and click on 'Your Profile.' An interface will then appear, allowing you to modify various information such as the password, name, or phone number.

“Ultimate Beneficial Owners” or “UBOs” refer to Individuals who directly or indirectly own or control a company. They are the actual economic beneficiaries of the company’s activities and decisions.

"**Account Manager**" refers to an SBS employee responsible for creating the Customer's account, handling Customer requests, monitoring consumption with the Customer, and checking invoices sent to the Customer based on recorded usage.

“**Owner**” refers to the Customer’s Authorized User responsible for setting up the Customer's account and managing the Customer's Authorized Users. Among the Customer's Authorized Users, at least one Owner must be defined.