SAP Ariba

Feature at a Glance

Risk Category Information API for Supplier Risk Exposure

Lisa Gangewere, SAP Ariba
Target GA: February 2021

Feature at a Glance

Ease of implementation High Touch
Geographic relevance Global

Introducing: **Risk Category Information API for Supplier Risk Exposure**

Customer challenge

Tracking and alerting for risk compliance violations is a core tenet of the SAP Ariba Risk platform. Currently, SAP Ariba Supplier Risk allows customers to bring in Watchlist and Sanction screening data via a single 3rd party licensed provider integration.

Complex organizations require more options for data sources, and Compliance Officers want to ensure that any compliance violations immediately flag a supplier as high risk.

Meet that challenge with SAP Ariba

A new external API allows customers to bring in compliance information such as Sanction and Watchlist violation screening results - with supporting evidence information - into Supplier Risk from a home grown system or a compliance partner of their choice.

Sanction and watchlist fields are introduced as standard fields in the risk configuration. Violations will be set as a default setting with a weight of *high* for the risk exposure calculation. When suppliers are screened and have sanction or watchlist violations, overall and the legal and regulatory exposure can be configured to be high (100).

Sanctions and Watchlist screening information that is brought in via this API will be now presented in a new regulatory and legal tab within the supplier profile.

Experience key benefits

Customers now have the flexibility to include a variety of data sources in their SAP Ariba Risk application - including data from standard and add-on licensed providers plus custom fields through the external API.

Sanction and watchlist violations are now standard fields, contributing to the risk exposure and mapped to the legal and regulatory risk category.

By default, sanction and watchlist violations will influence risk exposure to high risk (100) with the setting of the exposure override field (see ARI-13242).

Compliance information now readily visible in a new regulatory and legal tab within the supplier profile.

Solution area

SAP Ariba Supplier Risk
SAP Ariba APIs
SAP Ariba Developer Portal

Implementation information

This feature is **automatically on** for all customers with the applicable solutions and is ready for immediate use.

Prerequisites and Restrictions

The customer must have an entitlement to SAP Ariba Supplier Risk.

Feature at a Glance

Introducing: **Risk Category Information API for Supplier Risk Exposure**

Customer implementation teams will enable this feature through a series of three tasks:

Step 1: Risk configuration:

- The Supplier Risk Manager must create and activate a new draft of the risk configurator. This will present the new fields for sanction, watchlist and exposure override. These fields will have default settings for the exposure override field. This activation must be completed prior to pushing any supplier level data via the Risk Category Information API for Supplier Risk Exposure.
- The *weight* field for sanction and watchlist is set to HIGH by default.
- When utilizing the exposure override (see ARI-13242), the corresponding risk category MUST be contributing to the risk exposure. The category weight must be set to 1% or higher.

Step 2: Risk category information API for supplier risk exposure API configuration:

- Log into the developer portal to access the API: https://developer.ariba.com/api/ - users can log into their existing account or create a new account by following the login instructions
- SM VENDORID is the unique identifier that is required to import supplier-level information via the Risk Category Information API for Supplier Risk Exposure. The customer must identify suppliers via the SM VENDORID. Several options exist for exporting SM VENDORIDs
    - The Supplier Data API with Pagination can be utilized to retrieve valid supplier SM Vendor IDs.
    - A manual CSV export process from SM Admin area creates a file to identify suppliers and their SM VENDOR IDS
    - SLP customers may use the Manage->Supplier Data Snapshots to download the onboarding report which contains all vendor ids as well
- The information you submit in the Risk Category Information API for Supplier Risk Exposure cannot include personal information (such as personal phone numbers) or sensitive personal information (such as birth dates, government ID, or financial account numbers assigned to individuals). You can only submit publicly available business information.

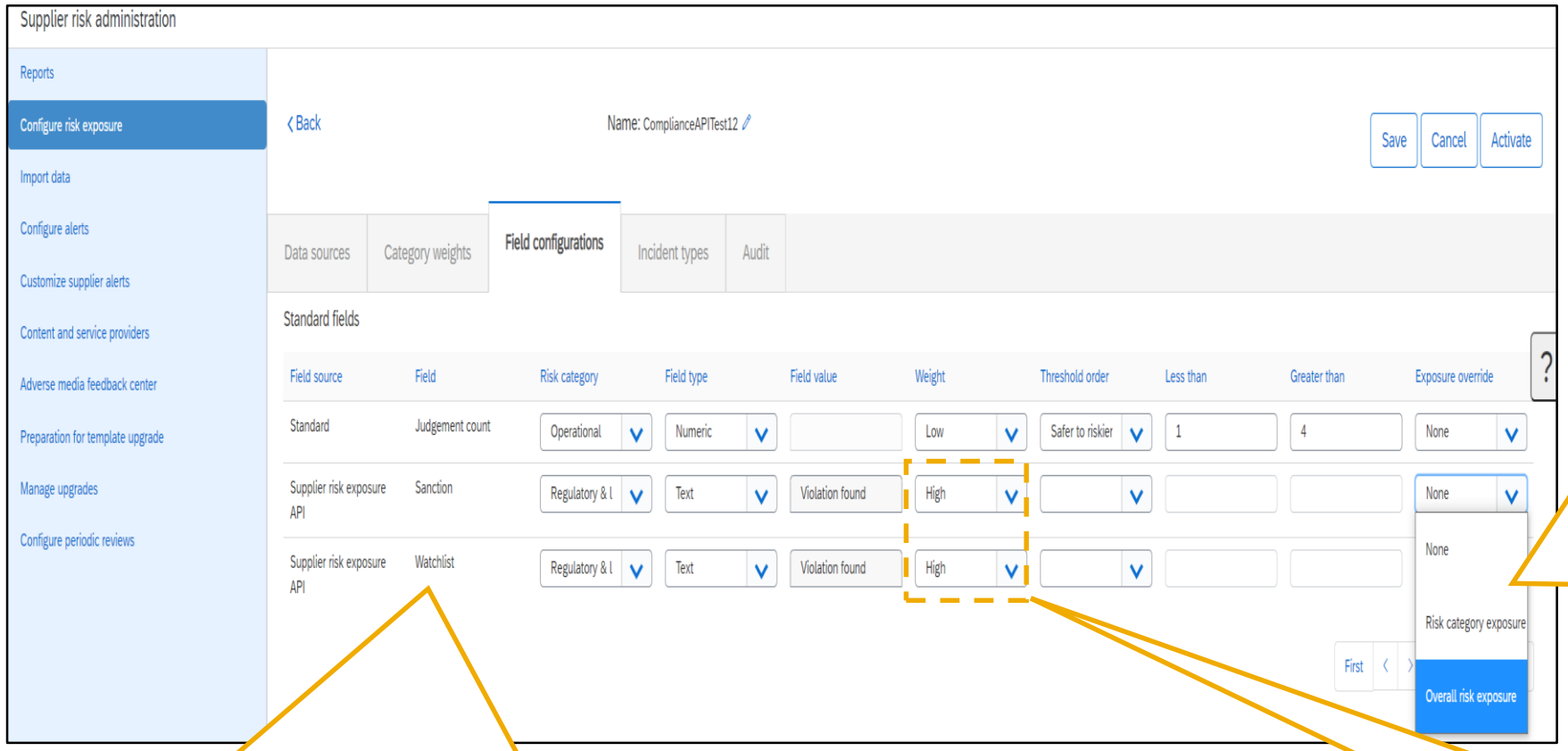
Step 3: Display of data in the Supplier Risk user interface:

- Compliance information imported via API will be presented in the SAP Ariba Risk user interface on a new Regulatory and Legal tab
- Sanction and/or watchlist violations will be contributing factors and listed in the risk exposure tab of the supplier profile
- Based on the default settings of the risk exposure, sanction and/or watchlist violations will drive the risk exposure to a High exposure (100) for the suppliers with violations

Step 1: Configure Risk Exposure

Feature at a Glance

Introducing: **Risk Category Information API for Supplier Risk Exposure**



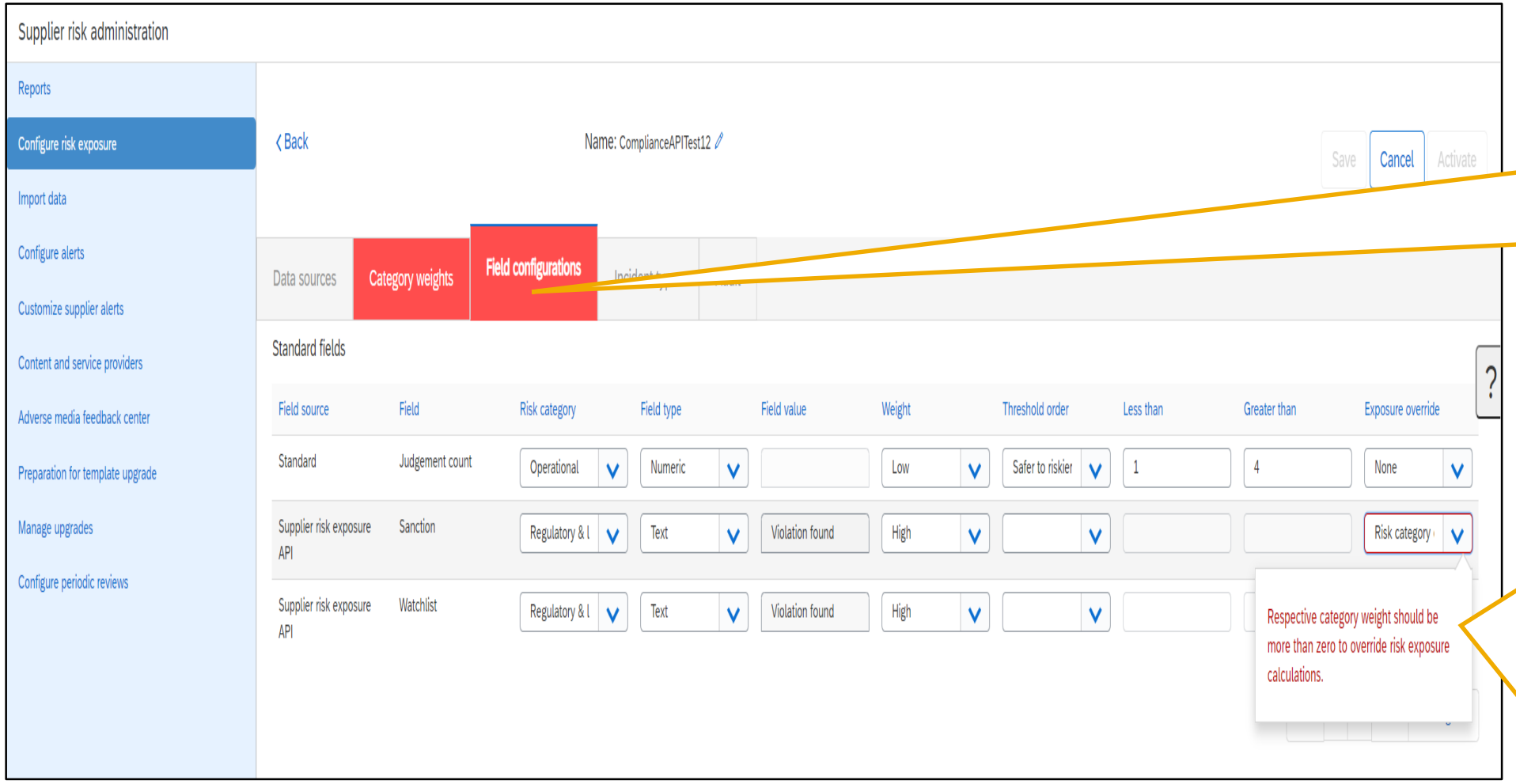
- A new Exposure feature is introduced; which overrides the standard exposure calculation when selected.
  - Select from the Overall risk exposure or Risk category exposure options
- By default, Sanction and Watchlist field exposure override is set to Overall exposure.
  - Overall risk exposure will set the Overall and Category exposure to HIGH when the supplier has a contributing factor of high risk.
  - Risk Category exposure will set the category only exposure to HIGH.

- As a first step, the Risk Manager should create a new draft of the risk configurator to display the new standard sanction and watchlist fields and the exposure override field.
- Sanction and watchlist fields have been introduced as standard fields to the risk configurations and are mapped to the Regulatory and legal risk category.

Weight is set to HIGH; this is a required setting when selecting the exposure override field. This will impact the exposure to 100.

Feature at a Glance

Introducing: **Risk Category Information API for Supplier Risk Exposure**

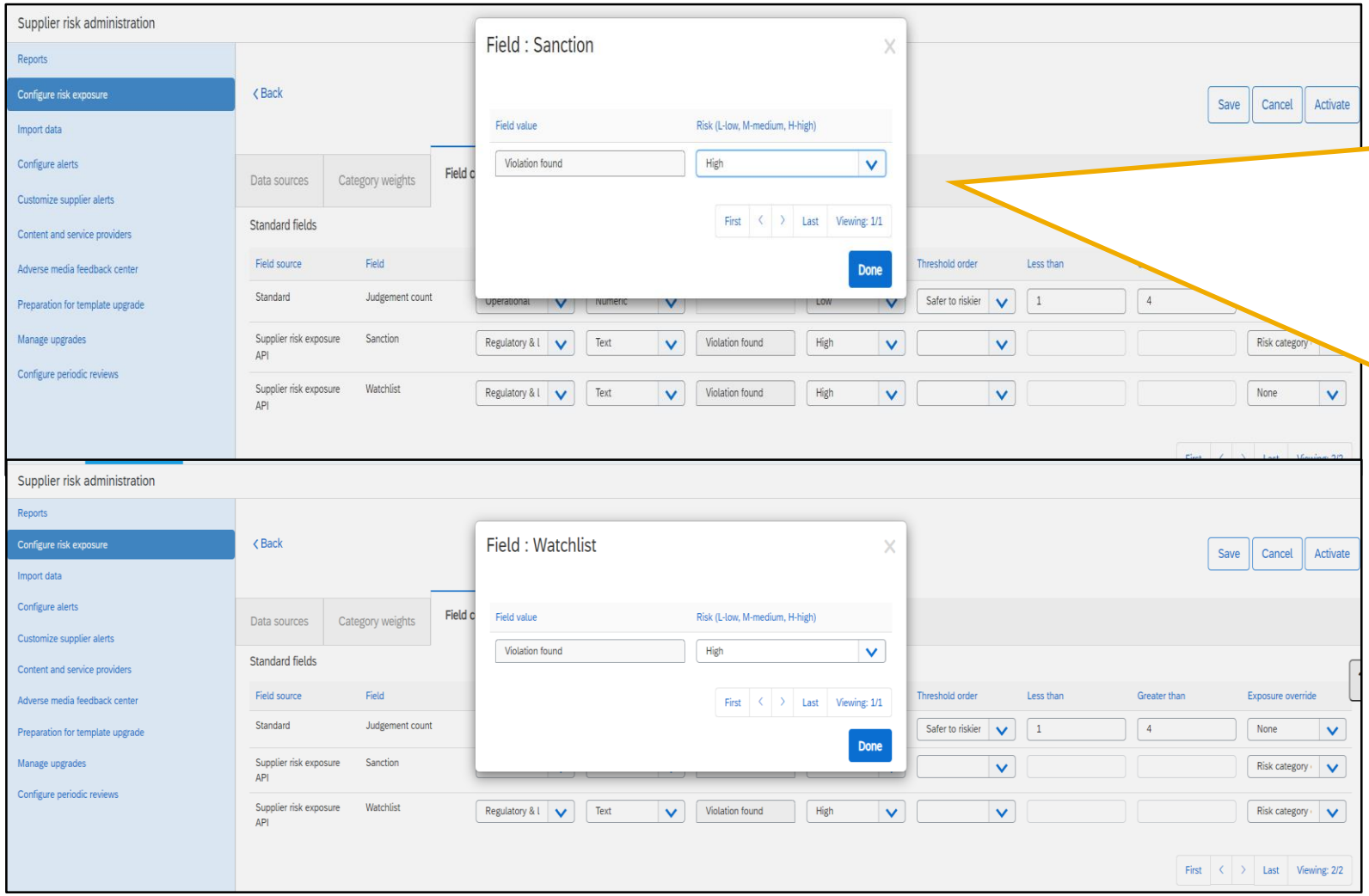


- When settings are not correct Risk managers will see the respective tab turn Red.
- The error must be corrected before the version of the risk configuration can be save and activated.

- When setting the exposure override field, the corresponding risk category MUST be contributing to the risk exposure on the Category Weight tab.
- The Regulatory and legal category must have a weight of at least 1%.
- The error may appear on the second page of the standard fields; user may need to view page 2/2 to view error.

Feature at a Glance

Introducing: **Risk Category Information API for Supplier Risk Exposure**



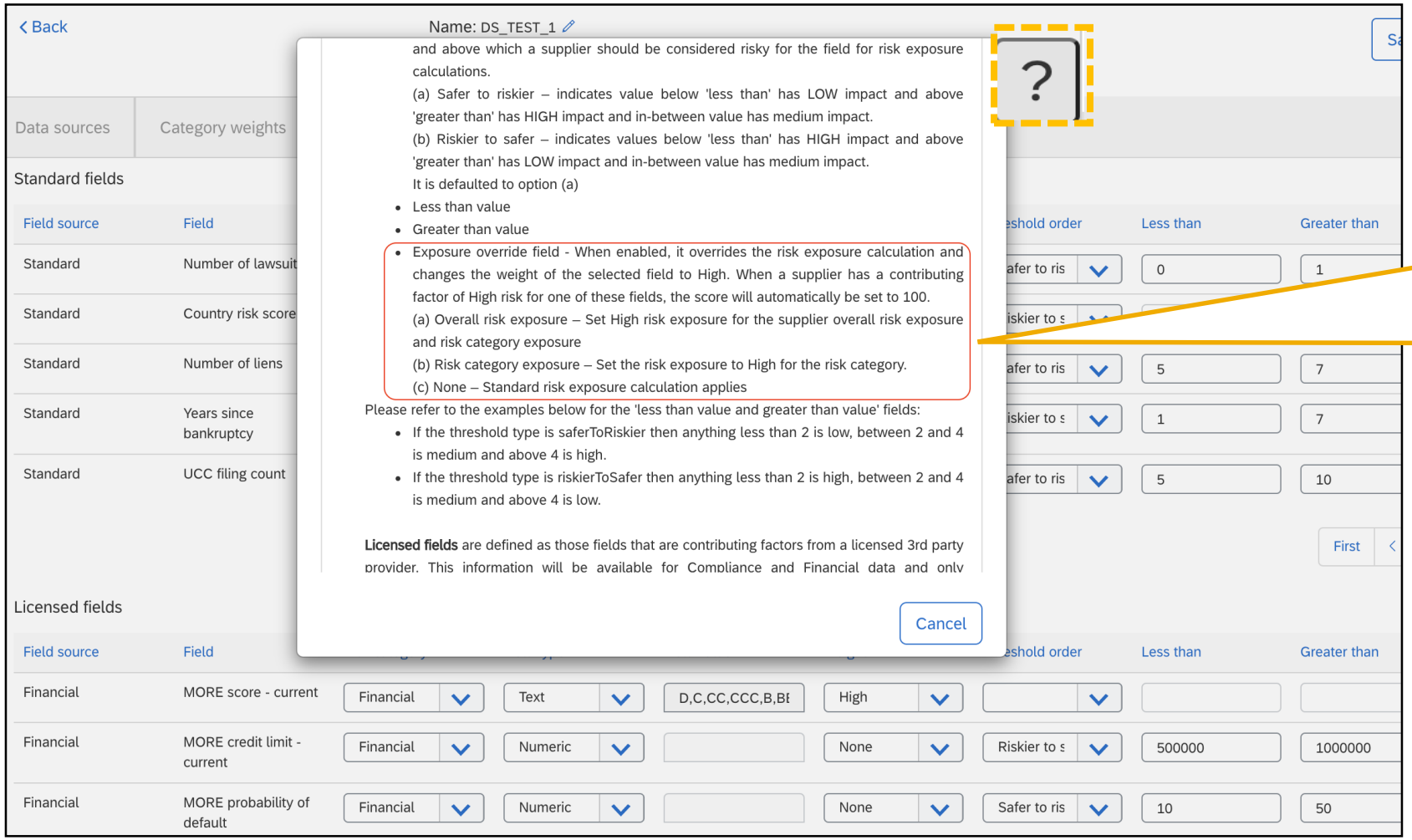
Sanction and watchlist fields are preset to one of the available 4 values. Sanction and watchlist violations are the only contributor to the risk exposure and are set as the default contributing factor with a high influence to the risk exposure. This High weight cannot be changed.

The 4 values that a buyer can provide for compliance screening are listed here. This information will be presented in the regulatory and legal tab of the supplier profile.

- **Violation found-** supplier screened and a violation of sanction or watchlist was found. This scenario impacts risk exposure with High weight by default.
- **Violation not found-** supplier was screened but no violation of a sanction or watchlist was found. There is no impact to risk exposure for this status.
- **Supplier screened and not found-** the supplier was screened but the entity was not found in the database. There is no impact to risk exposure for this status.
- **Supplier not screened-** the buyer has not screened the supplier for compliance violations. There is no impact to risk exposure for this status.

Feature at a Glance

Introducing: **Risk Category Information API for Supplier Risk Exposure**

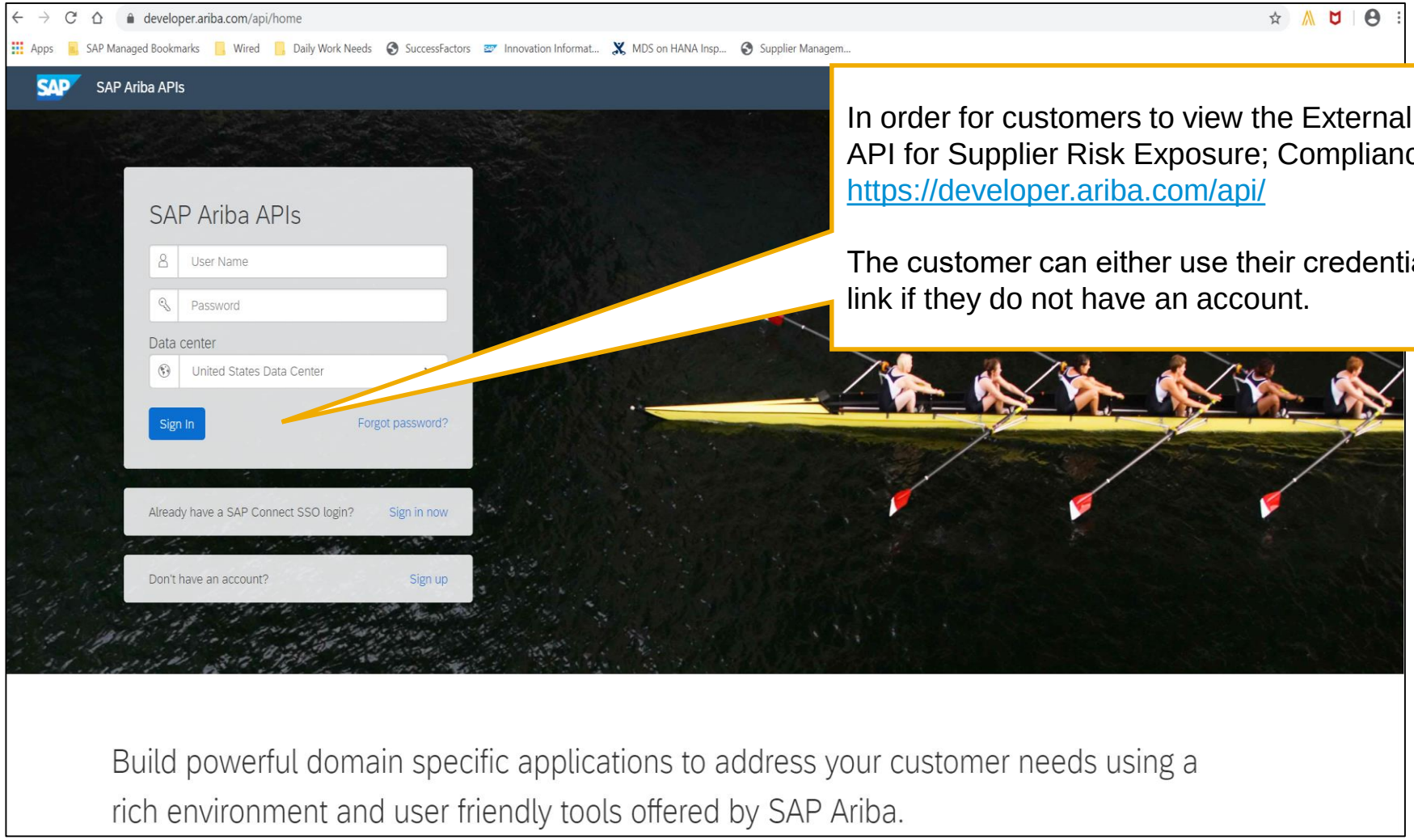


- When a user clicks the ? the help information screen opens where a user can access information about any tab of the risk configuration.
- The exposure override information has been added to the standard fields, licensed fields and custom field section in online help information section.

Step 2:
Configure Risk Category Information API for Supplier Risk Exposure – Get smVendorId

Feature at a Glance

Introducing: **Risk Category Information API for Supplier Risk Exposure**

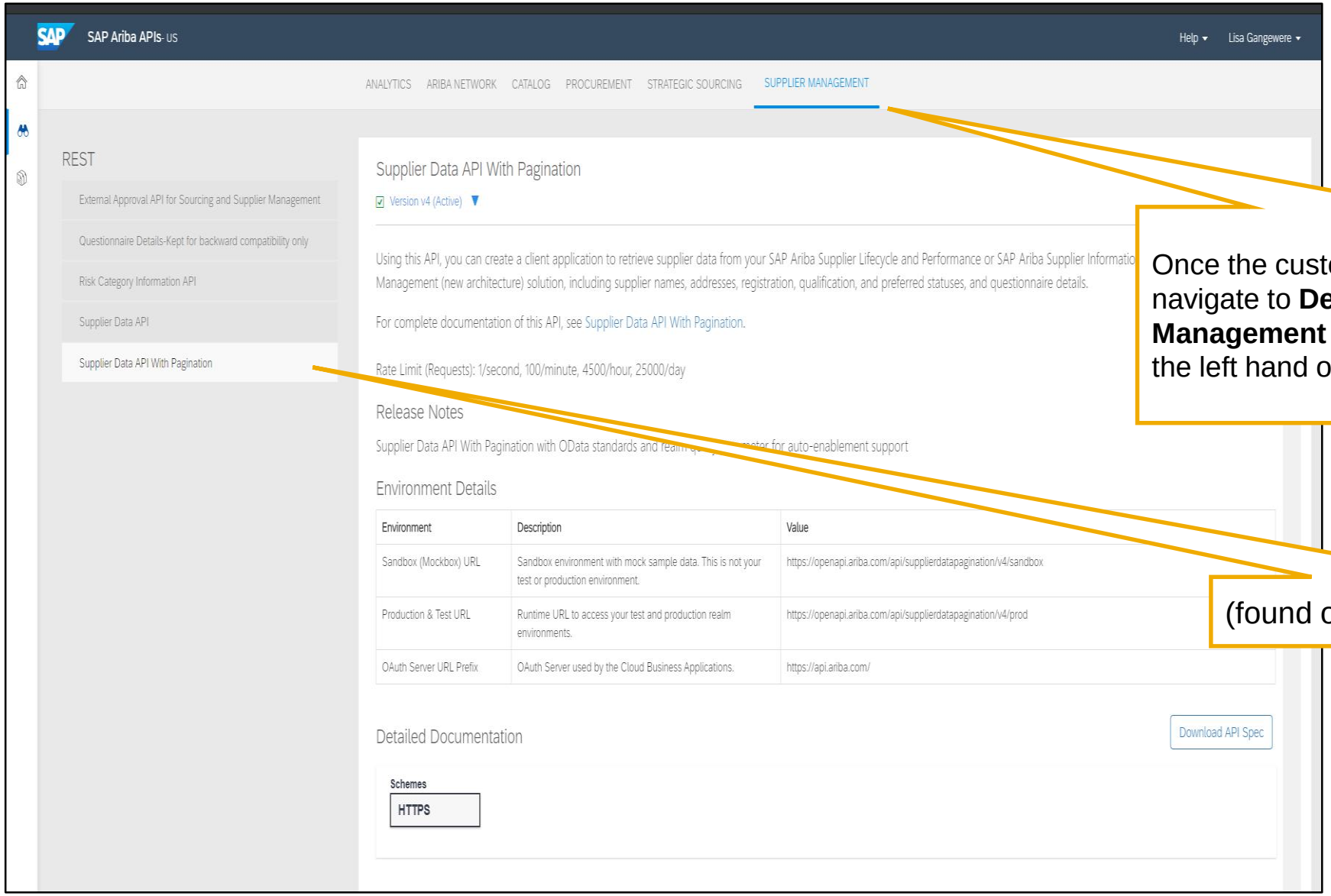


In order for customers to view the External API; Risk Category Information API for Supplier Risk Exposure; Compliance, they should use this link: https://developer.ariba.com/api/

The customer can either use their credentials to log in, or click the “sign up” link if they do not have an account.

Feature at a Glance

Introducing: **Risk Category Information API for Supplier Risk Exposure**

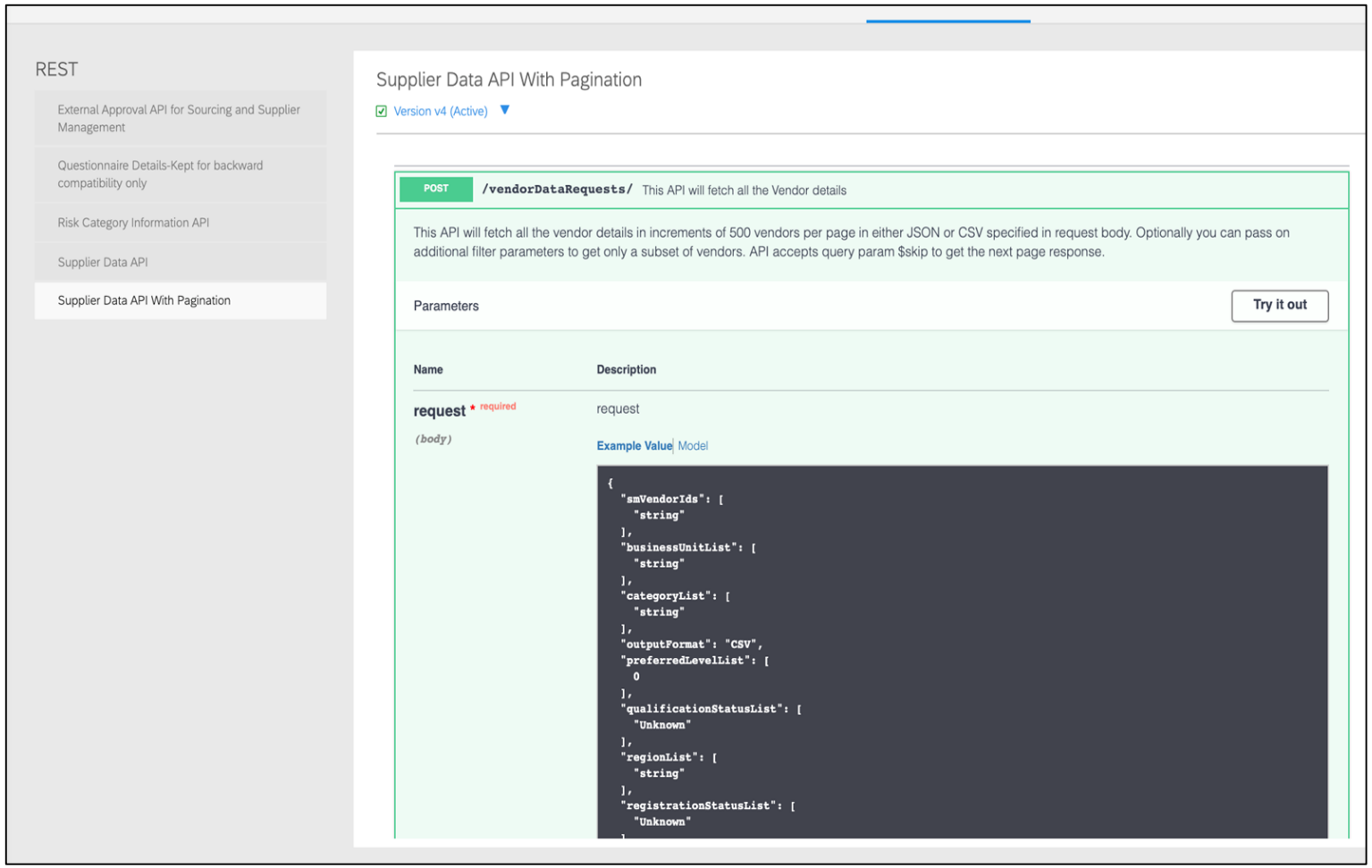


Once the customer has signed in, they should navigate to **Developer Area -> Supplier Management** to view the available APIs (found on the left hand of the screen)

(found on the left hand of the screen)

Feature at a Glance

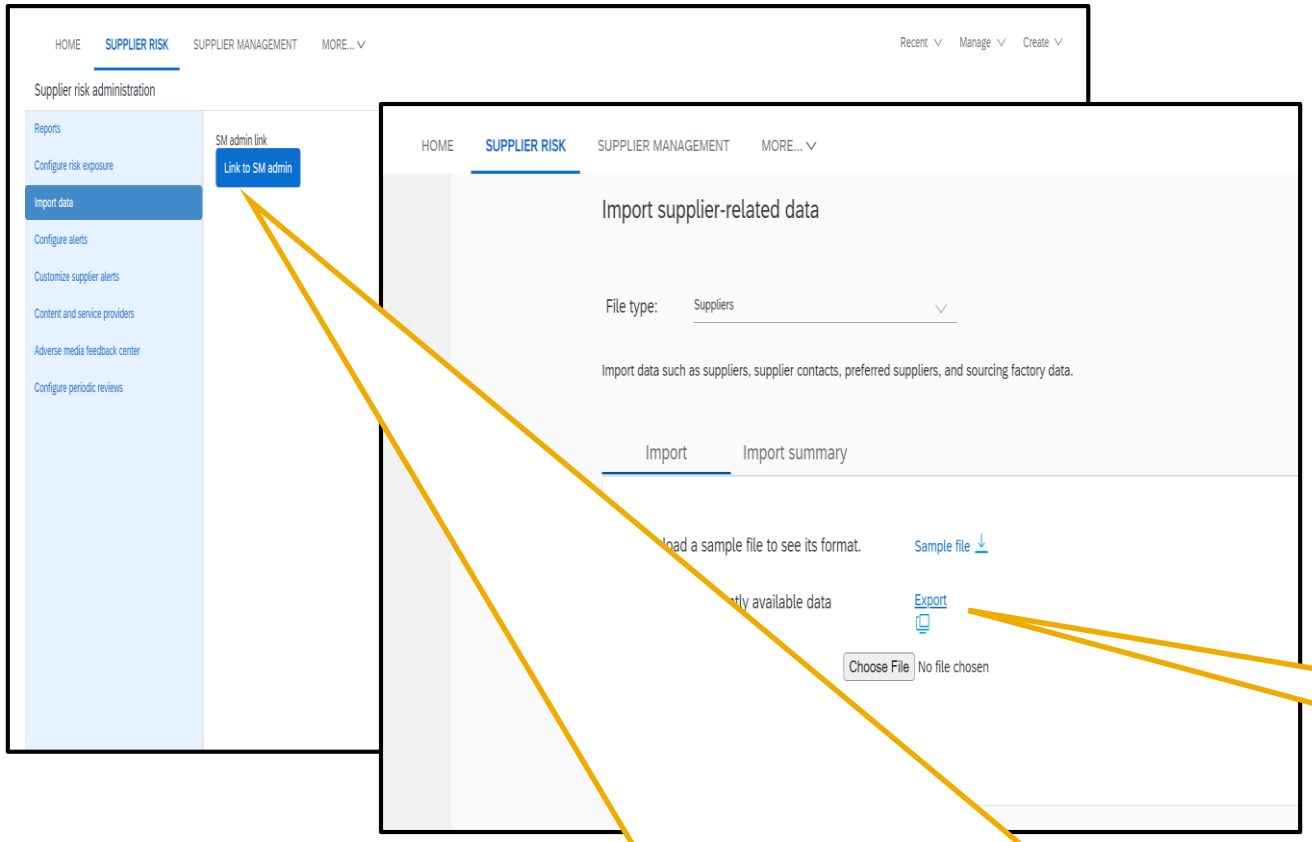
Introducing: **Risk Category Information API for Supplier Risk Exposure**



- **Supplier Data API with Pagination**: Using this API, you can create a client application to retrieve supplier data from your SAP Ariba Supplier Lifecycle and Performance or SAP Ariba Supplier Information and Performance Management (new architecture) solution, including supplier names, addresses, registration, qualification, and preferred statuses, and questionnaire details.
- Once the customer has signed in, they should navigate to **Developer Area -> Supplier Management** to view the available APIs (found on the left hand of the screen). The Supplier Data API with Pagination is displayed
- SM VENDORID is the unique identifier that is required to push supplier level information via the Risk Category information API for Supplier Risk Exposure.
- The Supplier Data API with Pagination should be utilized to fetch supplier SM Vendor ID.

Feature at a Glance

Introducing: **Risk Category Information API for Supplier Risk Exposure**



A customer may also manually create an export CSV file to obtain a list of all suppliers and their SM VENDOR ID's from their realm.

From the dashboard, navigate to **SM Administration**. Available paths depend on the groups to which your user belongs.

In sites that include **SM Administration**, members of the **SM Ops Administrator**, **SM ERP Admin**, or **Customer Administrator** group can select **Manage SM Administration**.

Members of the **Supplier Risk Manager** group can access **SM Administration** from the SAP Ariba Supplier Risk dashboard:

click the gear-shaped settings icon, then choose **Import data Link to SM admin**.

- Click **Export** to generate a CSV file.
- You can find the SM vendor ID for each vendor in this file.

- Click **Data import or export**.
- Depending whether you use SLP or SIPM, from the **File type** dropdown choose one of the following:
  - If you use SLP, choose **Suppliers**.
  - If you use SIPM, choose **Suppliers from Sourcing**

Feature at a Glance

Introducing: **Risk Category Information API for Supplier Risk Exposure**

SLP customers may use the Manage->Supplier Data Snapshots to download the onboarding report which contains all vendor ids.

Please access the information links below for detailed information related to the Supplier Data Snapshot report

- **How to run supplier onboarding supplier reporting**:
https://help.sap.com/viewer/f081c6c38fb7466a84d746a7998bfe0e/cloud/en-US/00736bc3df2944ad9bed8815cb7df76a.html

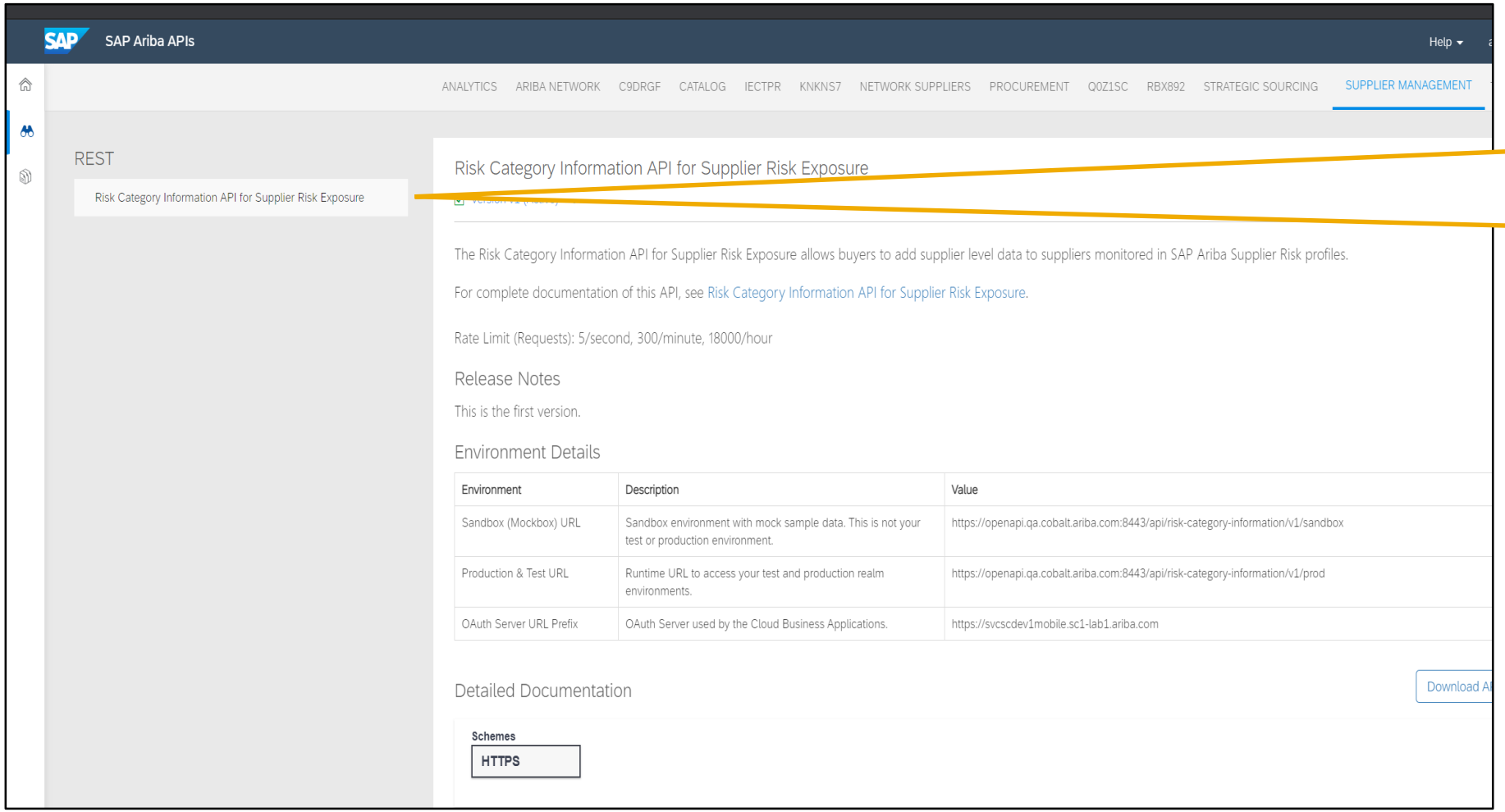
- **Supplier Onboarding Progress report reference**:
https://help.sap.com/viewer/f081c6c38fb7466a84d746a7998bfe0e/LATEST/en-US/cb16676b27f04624b9d6cac0fd588924.html

Step 2:
Configure Risk Category Information API for Supplier Risk Exposure – access Risk Category Information API

Feature at a Glance

Introducing: **Risk Category Information API for Supplier Risk Exposure**

The Risk Category Information API for Supplier Risk Exposure allows buyers to add supplier level data to suppliers monitored in SAP Ariba Supplier Risk profiles.



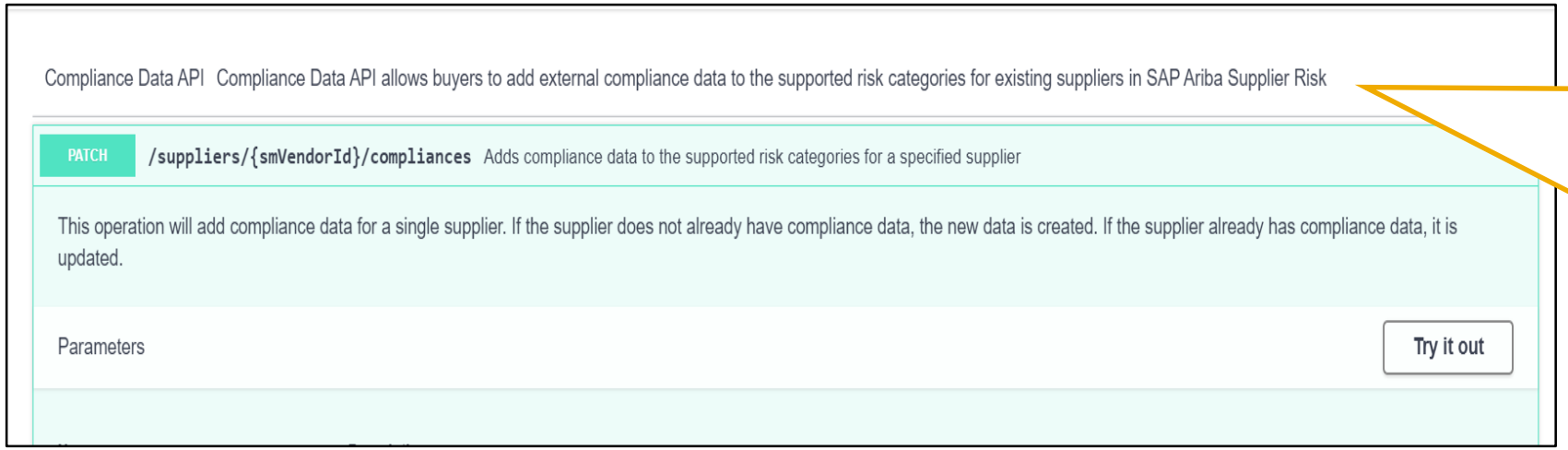
- Once the customer has signed in, they should navigate to **Developer Area -> Supplier Management** to view the available APIs (found on the left hand of the screen). The Risk Category Information API for Supplier Risk Exposure is displayed.

Note: With the release of the Risk Category Information API for Supplier Risk Exposure, the Risk Category Information API is deprecated.

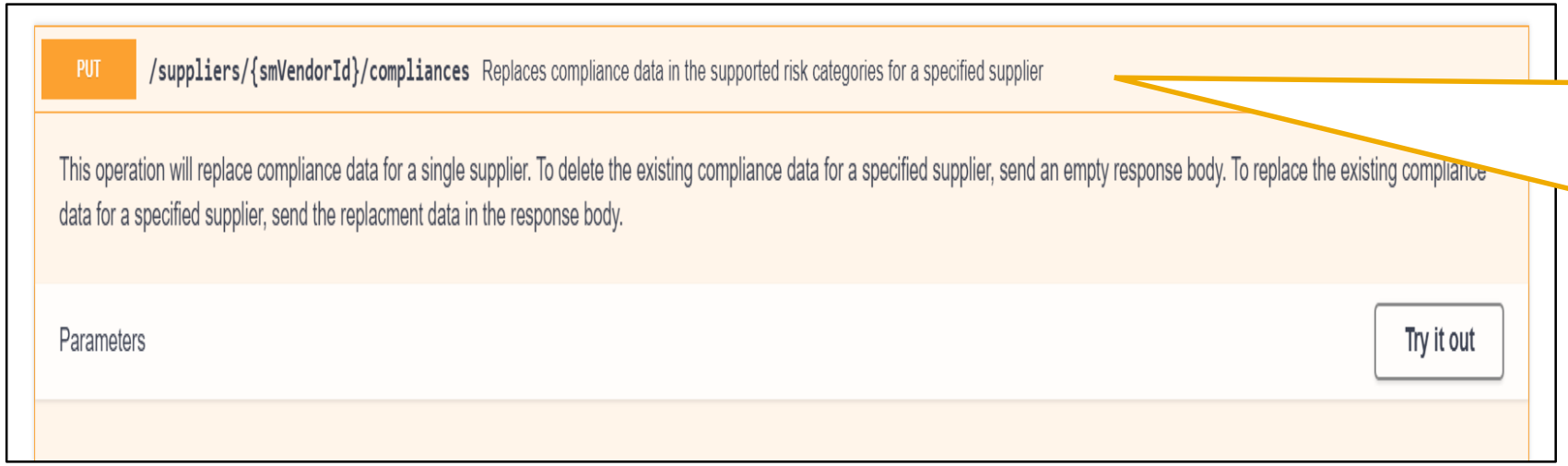
Please begin migrating any applications deprecated APIs or versions to version 1 of the Risk Category Information API for Supplier Risk Exposure instead.

Feature at a Glance

Introducing: **Risk Category Information API for Supplier Risk Exposure**



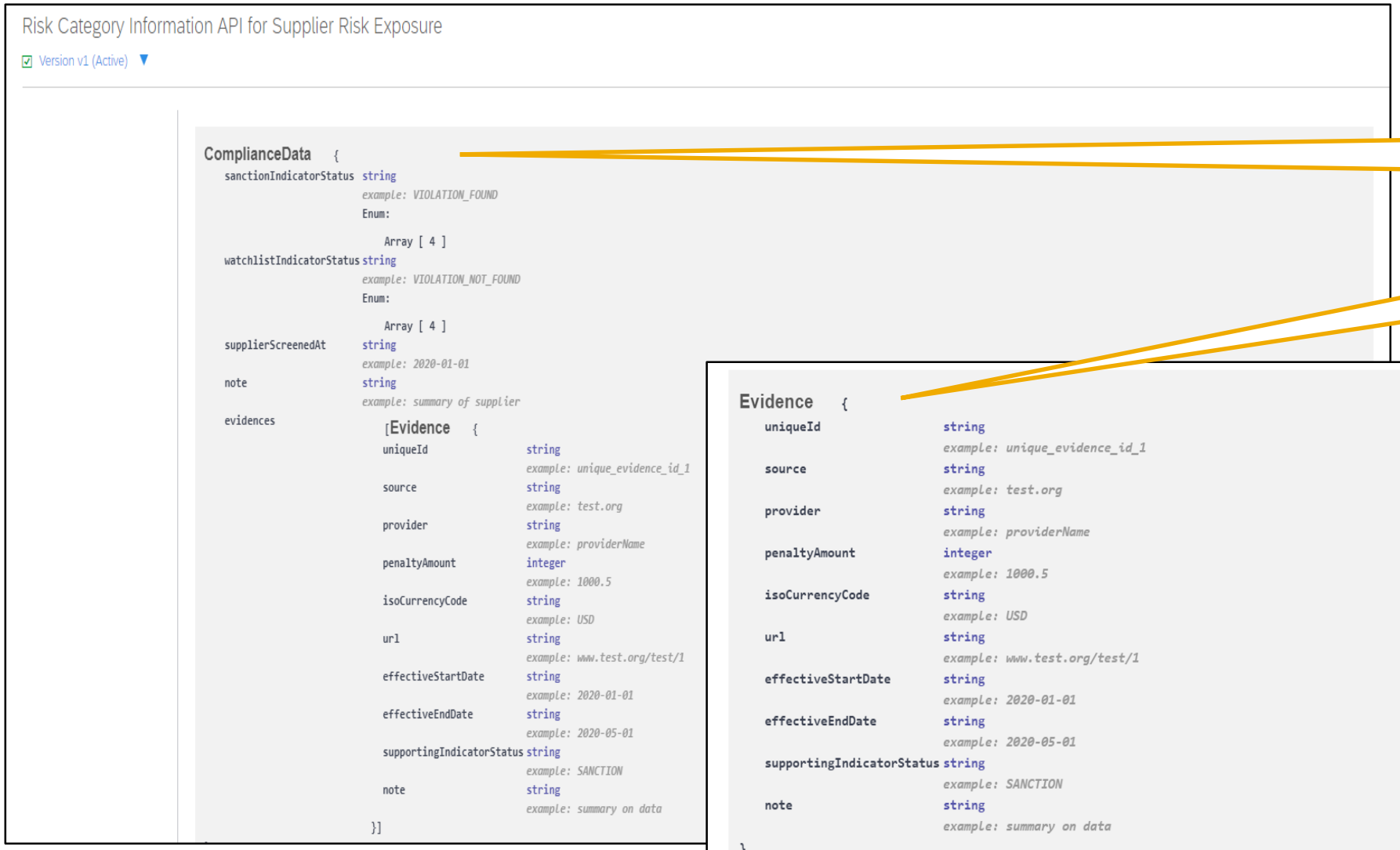
- This operation will add compliance data for a single supplier.
- If the supplier does not already have compliance data, the new data is created.
- If the supplier already has compliance data, it is updated.
- There are some mandatory fields required to import supplier data – Realm name, Smvendorid and compliance data.



- This operation will replace compliance data for a single supplier.
- To delete the existing compliance data for the specified supplier, send an empty request body.
- To replace the existing compliance data for a specified supplier, send the replacement data in the response body.

Feature at a Glance

Introducing: **Risk Category Information API for Supplier Risk Exposure**



This is an example of the compliance data field definitions format

This is an example of the evidence data definitions and format

Feature at a Glance

Introducing: **Risk Category Information API for Supplier Risk Exposure**

Detailed feature information

For help regarding how to use the SAP Ariba Developer Portal, including:

- How to set up user accounts/register applications for use on the developer portal
- Step-by-step instructions on how to create an application that consumes the APIs available
- How to incorporate the OAuth authentical portal

Please use the SAP Developer help guide found in the following link:

https://help.sap.com/viewer/b61dd8c7e22c4fe489f191f66b4c48d6/cloud/en-US/8907b13c87e240639be8f546251b1e35.html

Feature at a Glance

Introducing: **Risk Category Information API for Supplier Risk Exposure**

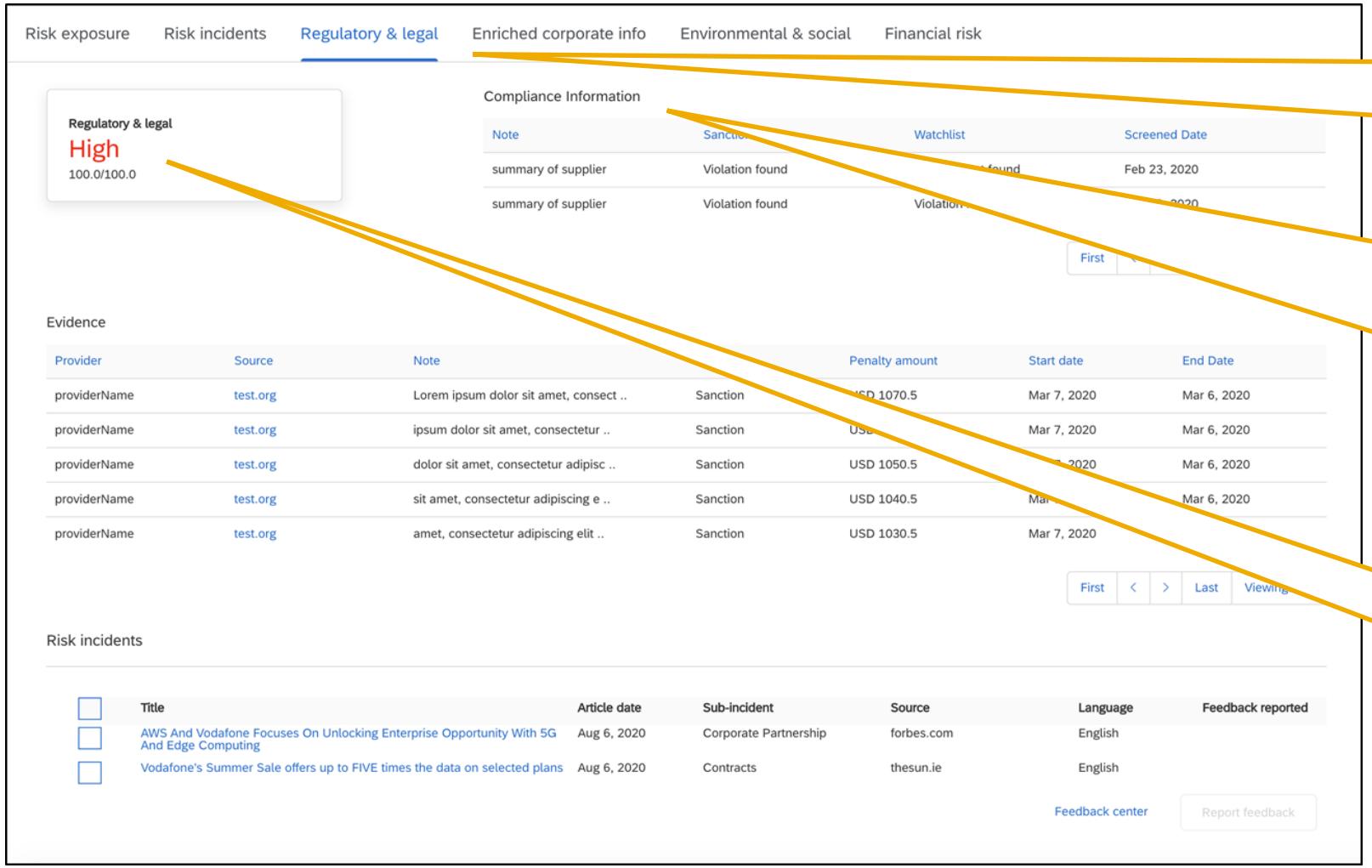
Here is a list of error messages that may be encountered when using this API. Use this information to troubleshoot your queries to the Risk Category Information API for Supplier Risk Exposure when updating compliance data.

Error code	Message	Description
400	`Realm name should not be empty`	The query URL doesn't specify your realm. Construct a new query URL including the realm name and retry your request.
400	`Body for PATCH cannot be null / empty`	Your JSON request body must have data. `PATCH` creates compliance data for suppliers that don't have any, and updates compliance data for suppliers that already have some.
400	`Could not find supplier with smVendorId XXX in realm YYY`	The specified realm doesn't contain a supplier with the specified SM Vendor ID. Check to make sure the specified realm name and smVendorID are correct, then resubmit your request.
400	`You cannot submit more than 100 evidences at a time`	Your JSON request body specifies too much evidence. The maximum amount of evidence for compliance data in a single request is 100. Split your request into multiple requests with no more evidence than 100.
400	`Please check the value of sanctionIndicatorStatus, value should not be null/empty. Accepted values are: VIOLATION_FOUND, VIOLATION_NOT_FOUND, VIOLATION_EXPIRED, NOT_SCREENED.`	Your JSON request body is missing the status that tells you if a `SANCTION` was found for the supplier. Add one of the accepted values.
400	`Please check the value of watchlistIndicatorStatus, value should not be null/empty. Accepted values are: VIOLATION_FOUND, VIOLATION_NOT_FOUND, VIOLATION_EXPIRED, NOT_SCREENED.`	Your JSON request body is missing the status that tells you if the supplier is on a `WATCHLIST`. Add one of the accepted values.
400	`Invalid supplierScreenedAt. Required date format is yyyy-MM-dd`	Your JSON request body specifies an invalid date format for `supplierScreenedAt`. The valid date format is `yyyy-MM-dd`.
400	`Invalid effectiveStartDate. Required date format is yyyy-MM-dd`	Your JSON request body specifies an invalid date format for `effectiveStartDate`. The valid date format is `yyyy-MM-dd`.
400	`Invalid effectiveEndDate. Required date format is yyyy-MM-dd`	Your JSON request body specifies an invalid date format for `effectiveEndDate`. The valid date format is `yyyy-MM-dd`.
400	`Realm YYY in the request does not match with realms in the token. Available realms in token are 'AAA,BBB,CCC'`	The specified realm in your request doesn't match the list of realms from the token. Change the realm in your request to one of the available realms in the token.
400	`Realm YYY in the request is not available in SR.`	The specified realm in the request isn't available in your supplier risk system.
400	`Please check the realm in request. Realm value should not be null or empty.`	The specified realm in your request can't be empty. Add the realm in your request.
400	`Error parsing Json request body. Error at line: x column: y`	There's an error in the data of your JSON request body. Correct the data in the line and column location.
400	`supplierScreenedAt should not be a future date`	Your JSON request body specifies an invalid date for `supplierScreenedAt`. The date you screened the supplier for compliance data can't be in the future. Change the date and resubmit.
400	`Invalid parameter smVendorId`	The query URL has an incorrect `smVendorId`. Correct the SM Vendor ID and resubmit your request.
500	`Error deleting compliance data`	Resubmit your request later.
500	`Error inserting compliance data`	Resubmit your request later.

Step 3:
Data Displayed in the Supplier Risk User interface

Feature at a Glance

Introducing: **Risk Category Information API for Supplier Risk Exposure**



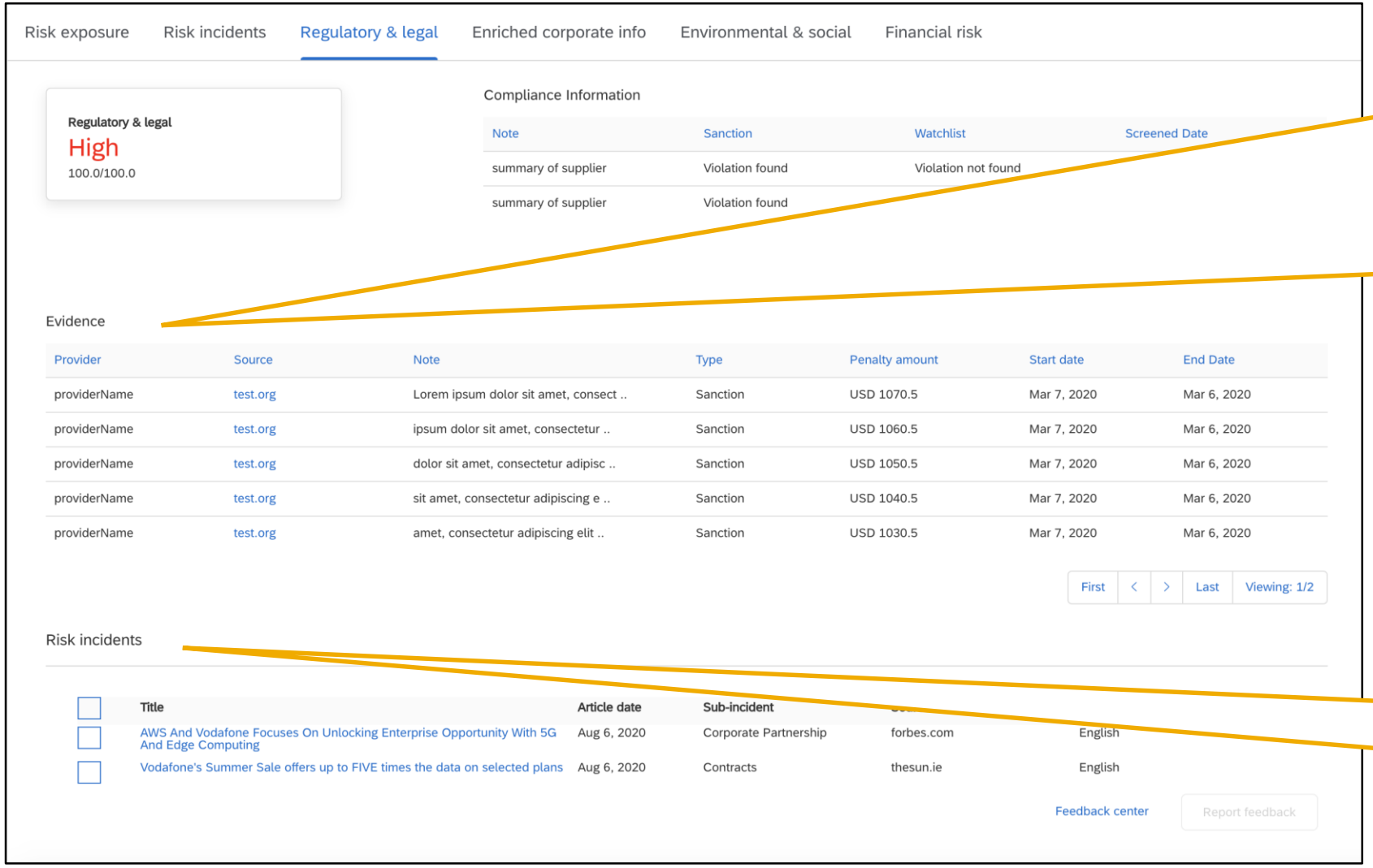
- A new Regulatory & legal tab was introduced to the Supplier profile
- This tile will include all compliance evidence information the buyer pushes into the supplier profile using the Risk Category Information API for Supplier Risk Exposure

- Compliance information area provides information that will allow the user to view a list of:
  - summary notes for the sanction and/or watchlist
  - Sanction detail
  - Watchlist detail
  - Screened at date which provides a date stamp of when the supplier was screened
- Over time the user will be able to access the history of the information that has been provided for each individual supplier.

- This Risk exposure represents the Regulatory & legal category exposure
- In this example, the exposure is HIGH because the supplier has a sanction and the override exposure field was set as a default

Feature at a Glance

Introducing: **Risk Category Information API for Supplier Risk Exposure**



The Evidence section of this tab summarizes the details supporting the sanction and/or watchlist for this supplier and is displaying information for reference.

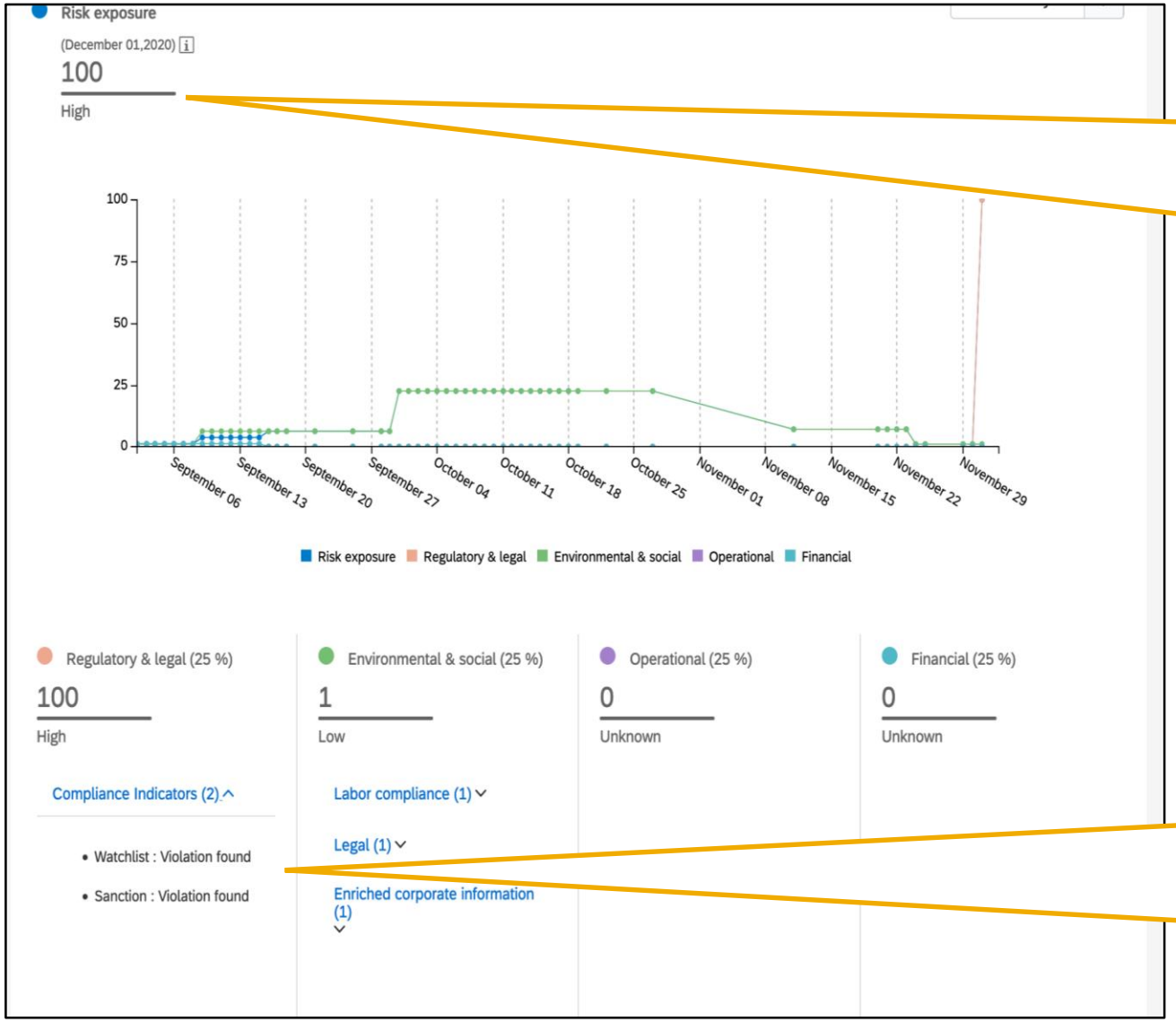
The data is not mandatory and therefore, if the buyer has not included information this section may be blank.

- **Provider-** source of the sanction/watchlist
- **URL -** a link that should start with http:// or https://".
- **Note-** this is a freeform field and will display 25 characters, the user can hover to see the popup for more information.
- **Start date -** if available, the date the violation began
- **End date -** if available, the date the violation ended.

The Risk incident section includes the adverse media that is mapped to the Regulatory and legal risk category. These are the same risk incidents that appear in the risk incidents tab of the supplier profile.

Feature at a Glance

Introducing: **Risk Category Information API for Supplier Risk Exposure**



- In this example, the overall Risk exposure is High (100) and Legal & regulatory exposure is High (100).
- Supplier has a violation.

The High risk exposure is generated The risk configuration default settings are set to:

- Sanction = High weight
- Watchlist = High weight
- Exposure override is defaulted to Overall

- A Sanction or Watchlist violation is a contributing factor since they are now a standard field in the risk configuration.
- When a supplier is screened with violation found, the Sanction or watchlist violation will be listed as a contributing factor to the Legal & regulatory risk category
- A user will be able to click the “Compliance Indicator” label and will be taken to the new regulatory and legal tab of the supplier profile to view the supporting evidence provided by the buyer.

Feature at a Glance

Introducing: **Risk Category Information API for Supplier Risk Exposure**

Subject: For your information: Supplier alerts and provider evaluation updates are available in SAP Ariba Supplier Risk

Adverse media alerts

Based on your supplier subscriptions, the below alerts are available for suppliers you are following.

Supplier name	Incident type	Severity	Received
United Parcel Service, Inc.	Regulatory Compliance Issue	High	June 1, 2020

Go To alerts in the **Alert feed** tile on the **Supplier Risk** dashboard.

Third-party provider

The suppliers you are following have been submitted for evaluation to a third-party provider. Below are the supplier evaluation updates from the provider.

Supplier name	Provider name	Risk category	Received
Xpo Logistics, Inc.	DNB	Financial	June 2, 2020

Risk Category Information API for Supplier Risk Exposure

The suppliers you are following have been updated with information provided by your buyer via the Risk Category Information API for Supplier Risk Exposure. Below are the suppliers that have been updated.

Supplier name	Risk category	Received
Xpo Logistics, Inc.	Legal and Regulatory	November 11, 2020

https://svcdev8ss.ariba.com/Sourcing/Main?realm=ERPCustomer to access the supplier 360° profile and see the evaluation updates.

Suppliers may have been inactivated in SAP Ariba Supplier Management by your organization. As a result, you may notice the following changes in your SAP Ariba Supplier Risk supplier subscriptions:

- Inactive suppliers have been removed from your dashboard
- Alert notification emails have been inactivated for these suppliers
- These suppliers are ineligible for submission for risk evaluation by a licensed provider

To see the list of inactive suppliers, please sign in to SAP Ariba Supplier Risk at https://svcdev8ss.ariba.com/Sourcing/Main?realm=ERPCustomer and select the inactive supplier status from the supplier list page in the dropdown.

Thank you,
SAP Ariba Supplier Risk

- Supplier Risk users who are following suppliers that are updated with Risk Category Information will receive information in the daily email notifications that the supplier has been updates with data from the Risk Category Information API for Supplier Risk Exposure

Feature at a Glance

Introducing: **Risk Category Information API for Supplier Risk Exposure**

Subject: For your information: Supplier alerts and provider evaluation updates are available in SAP Ariba Supplier Risk

Adverse media alerts

Based on your supplier subscriptions, the below alerts are available for suppliers you are following.

Supplier name	Incident type	Severity	Received
Sample Supplier 4	Regulatory Compliance Issue	High	December 14, 2020
Sample Supplier 5	Regulatory Compliance Issue	High	December 14, 2020
Sample Supplier 1	Complaint	Medium	December 15, 2020
Sample Supplier 2	Complaint	Medium	December 14, 2020

Low severity alerts are not included in this email but you can see them by clicking **Go To alerts** in the **Alert feed** tile on the **Supplier Risk** dashboard.

Third-party provider

Your Supplier Risk realm is enabled with licensed providers. The suppliers you are following have been submitted for evaluation however, there are currently no updates.

Supplier name	Provider name	Risk category	Received
No provider updates found.			

Risk Category Information API for Supplier Risk Exposure

The suppliers you are following have been updated with information provided by your buyer via the Risk Category Information API for Supplier Risk Exposure. Below are the suppliers that have been updated

Supplier name	Risk category	Received
Sample Supplier 1	Legal and Regulatory	December 15, 2020
Sample Supplier 2	Legal and Regulatory	December 15, 2020

You can also sign in to SAP Ariba Supplier Risk by clicking this link https://svcdev8ss.ariba.com/Sourcing/Main?realm=ERPCustomer to access the supplier 360° profile and see the evaluation updates.

Suppliers may have been inactivated in SAP Ariba Supplier Management by your organization. As a result, you may notice the following changes in your SAP Ariba Supplier Risk supplier subscriptions:

- Inactive suppliers have been removed from your dashboard
- Alert notification emails have been inactivated for these suppliers
- These suppliers are ineligible for submission for risk evaluation by a licensed provider

To see the list of inactive suppliers, please sign in to SAP Ariba Supplier Risk at https://svcdev8ss.ariba.com/Sourcing/Main?realm=ERPCustomer and select the inactive supplier status from the supplier list page in the dropdown.

Thank you,
SAP Ariba Supplier Risk

This is an automatically generated email. Please do not reply to this email.

- Supplier Risk users who are following suppliers that are updated with Risk Category Information will receive information in the daily email notifications that the supplier has been updates with data from the Risk Category Information API for Supplier Risk Exposure

Feature at a Glance

Introducing: **Risk Category Information API for Supplier Risk Exposure**

Detailed feature information and best practices

- As a first step, the Supplier Risk user with Risk Manager permissions should create a new draft of the risk configurator. This will present the standard Sanction and watchlist and Exposure override fields with the out of the box default settings for the exposure override field. This should be completed prior to importing any supplier level data via the Risk Category Information API for Supplier Risk Exposure.
- The weight field for sanction and watchlist is set to High by default but is configurable
- The override exposure field is on by default for the sanction and watchlist standard fields and set to Overall Exposure.
- When utilizing the exposure override the corresponding risk category MUST be contributing to the risk exposure – the category weight must be set to 1% or higher.
- In risk configuration, there are 2 pages of standard fields; if there is an error on the field settings tab of the risk configuration; the user should view page 2/2 to check for the possible error.
- To access the Risk Category Information API for Supplier Risk Exposure, Log into the developer portal to access the API: https://developer.ariba.com/api/
- When using the Risk Category Information API for Supplier Risk Exposure, the customer must identify suppliers via the SM Vendor ID. SM vendorid is the unique identifier when importing supplier level information
- The Supplier Data API with Pagination should be utilized to fetch supplier SM Vendor ID.
- Customers can also use a manual CSV export process from SM ADMIN to create a file to identify suppliers and SM VENDOR IDS.
- The information you submit in the Risk Category Information API for Supplier Risk Exposure cannot include personal information (such as personal phone numbers) or sensitive personal information (such as birth dates, government ID, or financial account numbers assigned to individuals). You can only submit publicly available business information.