



PUBLIC

Document Version: 2608 – 2026-08

Risk Category Information API for Supplier Risk Exposure

SAP Ariba APIs

SAP Ariba Developer Portal

SAP Ariba Supplier Risk

SAP Ariba Supplier Risk, base edition



Content

Risk Category Information API for Supplier Risk Exposure.	3
Overview of Custom Field Data in the Risk Category Information API for Supplier Risk Exposure.	5
Workflow for Custom Field Data in the Risk Category Information API for Supplier Risk Exposure.	6
Updating Supplier Custom Fields Using the Risk Category Information API for Supplier Risk Exposure	6
Risk Category Information API for Supplier Risk Exposure Custom Field Data Error Messages.	9
Overview of External Compliance Data in the Risk Category Information API for Supplier Risk Exposure.	11
Workflow for Compliance Data in the Risk Category Information API for Supplier Risk Exposure.	12
Updating Supplier Compliance Data Using the Risk Category Information API for Supplier Risk Exposure.	12
Risk Category Information API for Supplier Risk Exposure Compliance Data Error Messages.	16
Version History for the Risk Category Information API for Supplier Risk Exposure.	19
API-Specific Disclaimers and Legal Information.	20

Risk Category Information API for Supplier Risk Exposure

This guide is for application developers seeking information about how to build client applications to add supplier level data to suppliers monitored in risk profiles.

Buyers use risk category information to see the exposure trends for their current suppliers.

The Risk Category Information API has been renamed the Risk Category Information API for Supplier Risk Exposure.

Note

This guide only contains information about the active version of this API. To see which version of this API is the active version, see the version history.

This guide applies to:

- SAP Ariba Developer Portal
- SAP Ariba APIs
- SAP Ariba Supplier Risk
- SAP Ariba Supplier Risk, base edition

Restrictions

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.

Related Guides

[Supplier Data API with Pagination](#)

[Risk Exposure API](#)

[Supplier Risk Engagements API](#)

[Setting Up SAP Ariba Supplier Risk](#)

[Help for the SAP Ariba Developer Portal](#)

Related Information

[Running the Risk Category Information API Report](#)

Overview of Custom Field Data in the Risk Category Information API for Supplier Risk Exposure

The Risk Category Information API for Supplier Risk Exposure allows you to import supplier custom field data to the suppliers monitored in risk profiles.

Client applications construct API queries that update the values of specified custom supplier fields in SAP Ariba Supplier Risk. SAP Ariba Supplier Risk allows customers to add up to 300 custom fields to their risk exposure configuration for each supplier. The values for these custom fields can still be updated using the existing CSV-file upload process. However, by using the Risk Category Information API for Supplier Risk Exposure, custom field values can be added programmatically rather than manually uploading a CSV file.

Note

The manual CSV upload process identifies each supplier by ERP Vendor ID and source system. When you use the Risk Category Information API for Supplier Risk Exposure, you must use the SM Vendor ID instead.

This API includes the following custom field data endpoints:

PATCH /suppliers Imports values specified in the query body into the custom fields configured in SAP Ariba Supplier Risk.

Prerequisites

- To create an application and request access to use this API, you must have access to the SAP Ariba Developer Portal. For details refer to [Steps to Start Using the SAP Ariba APIs in Help for the SAP Ariba Developer Portal](#).
- All queries made to this API must be authenticated using OAuth authentication. For details refer to [SAP Ariba Developer Portal Authentication in Help for the SAP Ariba Developer Portal](#).
- Before adding custom fields to your SAP Ariba Supplier Risk configuration, you must first determine the SM Vendor IDs of all relevant suppliers.
- Best practice is to set up custom fields in the SAP Ariba Supplier Risk configuration interface before executing your API updates. For details see [Setting Values and Risk Exposures for Fields in Setting Up SAP Ariba Supplier Risk](#).

Restrictions

This API can be used to update custom fields for a maximum of 100 suppliers per request.

When configuring custom fields in the user interface or populating custom fields with values in the API, best practice is never to include personally identifiable information (PII) in custom fields.

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.

Workflow for Custom Field Data in the Risk Category Information API for Supplier Risk Exposure

Use the Risk Category Information API for Supplier Risk Exposure to update the values of supplier custom fields.

1. If not already done, a customer administrator configures the SAP Ariba Supplier Risk risk configuration with the names of the custom fields, and the weight each field will have for the calculation of each supplier's risk exposure. The configuration interface allows you to add up to 300 custom fields. For details see [Setting Values and Risk Exposures for Fields](#) in [Setting Up SAP Ariba Supplier Risk](#).
2. The customer identifies the SM Vendor ID for each desired supplier. This is used to map suppliers to their custom fields.
3. The client application or a customer developer constructs a JSON request body that provides the values of custom fields for each supplier, identified by SM Vendor ID.
4. The client application passes this JSON to the API to update the SAP Ariba Supplier Risk risk configuration with the values for each supplier's custom fields.

Updating Supplier Custom Fields Using the Risk Category Information API for Supplier Risk Exposure

Use these steps to add custom field data to the existing suppliers in your risk solution.

Prerequisites

1. Best practice is to [create a new draft version in the configuration editor](#), create your custom fields, and activate the draft version before executing your API updates. The configuration interface allows you to add up to 300 custom fields. The custom fields can contribute to the risk exposure, or they can be displayed as information only and not contribute to the risk exposure.
2. For each supplier, determine the SM Vendor ID as follows:
 1. 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**.

Note

Members of the **Supplier Risk Manager** group must also be members of the **SM Ops Administrator** group.

2. Click **Data import or export**.
3. 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**.
4. Click **Export** to generate a CSV file. You can find the SM vendor ID for each vendor in this file.

Context

Once your SAP Ariba Supplier Risk configuration is complete and you have the SM Vendor IDs of all relevant suppliers, construct a client application as follows to update supplier custom field values.

Note

In the sample URLs in this topic, replace `{{runtime_url}}` with the desired runtime URL from the **Environment Details** table on the SAP Ariba Developer Portal discovery page for this API.

Procedure

1. Construct a JSON query body to set the value for each supplier's custom fields, as follows:

```
"value": [
{
  "smVendorId": "vendor_id_1",
  "customFields": [
    {
      "fieldName": "FIELD_04",
      "value": "value_of_field_04"
    },
    {
      "fieldName": "FIELD_02",
      "value": "value_of_field_02"
    },
    ...
    {
      "fieldName": "FIELD_19",
      "value": "value_of_field_19"
    }
  ]
},
{
  "smVendorId": "vendor_id_N",
  "customFields": [
    {
      "fieldName": "FIELD_01",
      "value": "value_of_field_01"
    },
    ...
  ]
}
]
```

]

SMVendorId	The SM Vendor ID that identifies the specific supplier. You found this ID in the prerequisite steps above.
customFields	This block contains pairs of fieldName/value pairs that assign values to each custom field for the specified supplier.
fieldName	Identifies which custom field value belongs to. Field names can include letters, numbers, and underscore.
value	The value of the custom field specified in fieldName . Ensure that this value matches the data type of the custom field as configured in the UI.

Note

Specify values for the custom fields that you want to update. It isn't necessary to specify values for all custom fields when using the API or the manual CSV file upload. For example, if there are 5 custom fields in SAP Ariba Supplier Risk, and the API has values to update only the first custom field, it's not necessary to specify values for the other 4 custom fields. If you don't specify a value for custom fields, the values for those custom fields won't be updated.

2. Update the values of your suppliers' custom fields by using the **PATCH /suppliers** endpoint, passing the JSON body constructed earlier:

```
PATCH {{runtime_url}}/suppliers?realm=myRealm
{
  "value": [
    {
      "smVendorId": "Vendor123",
      "customFields": [
        {
          "fieldName": "FIELD_01",
          "value": "123454"
        }
      ]
    }
  ]
}
```

This query assigns the value of the Vendor123 custom field assigned to field 1 in the UI, replacing the current value, if any, with 123454. If additional custom fields have been configured for Vendor123, the values for those custom fields are erased. Remember to assign values to all relevant custom fields.

Results

On success, the response includes a 201 success code. Within SAP Ariba Supplier Risk the values specified in your **PATCH /suppliers** request are assigned to their respective custom fields. If you assign a new value to a custom field that already had a value, the new value replaces the old one.

On failure, the response includes an error message. See [Risk Category Information API for Supplier Risk Exposure Custom Field Data Error Messages \[page 9\]](#) for a list of possible errors.

Risk Category Information API for Supplier Risk Exposure Custom Field Data Error Messages

Use this information to troubleshoot your queries to the Risk Category Information API for Supplier Risk Exposure when adding custom field 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	The apikey passed in the request is not valid.	The API key passed in the query headers doesn't match the API key in the OAuth token.
400	You cannot submit more than 100 records at a time	The JSON body of your request specifies too many suppliers. The maximum number of suppliers whose custom fields you can update in a single request is 100. Split your request into multiple requests of 100 or fewer suppliers.
400	smVendorId should not be empty	One or more of the fieldName/value blocks in your JSON request body doesn't specify a value for the smVendorId . Ensure that all smVendorId fields have a valid SM Vendor ID, then resubmit your request.
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	CustomFields should not be empty for smVendorID XXX in realm YYY	The JSON body of your request doesn't specify any custom fields to be updated for the specified supplier. Add at least one fieldName/value pair to the CustomFields block for the specified vendor, then resubmit your request.
400	Too many custom fields specified for smVendorID XXX in realm YYY	The JSON body of your request specifies too many custom fields for the specified supplier. The maximum number of custom fields you can update for each supplier is 300. Delete extra fieldName/value pairs from the CustomFields block for the specified supplier, then resubmit your request.

Error Code	Message	Description
400	Duplicate fields name for smVendorID XXX in realm YYY: LIST_OF_DUPLICATE NAMES	Your JSON request body specifies a duplicate fieldName for the specified supplier. A fieldName can't be a duplicate of another fieldName for custom, licensed, or standard fields.
400	No field name for smVendorID XXX in realm YYY: FIELD_VALUE	Your JSON request body is missing a fieldName for the specified supplier and fieldValue . The fieldName can't be empty. Add a fieldName for the fieldValue .
400	No field value for smVendorID XXX in realm YYY: FIELD_NAME	Your JSON request body is missing a fieldValue for the specified supplier and fieldName . The fieldValue can't be empty. Add a fieldValue for the fieldName .
429	Rate limit error	You've exceeded the maximum permitted query rate. Refer to the developer portal discovery page for this API for the applicable query rates.
500	Error inserting custom fields data	Resubmit your request later.
504	Gateway Time-out	The server timeout time has been exceeded, possibly due to network traffic or reliability issues. Retry your query.

Overview of External Compliance Data in the Risk Category Information API for Supplier Risk Exposure

The Risk Category Information API for Supplier Risk Exposure allows you to import external compliance data based on supported risk categories to the suppliers monitored in risk profiles. You can then view the data on the applicable risk category tab in the supplier 360° profile.

Sanction and watchlist compliance data can be imported and used as a contributing factor to the supplier's risk exposure.

Sanction and watchlist data from the API is mapped to the **Regulatory & legal** risk category.

You can view the imported sanction and watchlist compliance data in the supplier 360° profile on the **Regulatory & legal** tab.

This API includes the following endpoints for external compliance data:

PATCH /suppliers/{smVendorId}/compliances	This endpoint adds compliance data for a single supplier. If the supplier doesn't already have compliance data, the new data is created. If the supplier already has compliance data, it's updated.
PUT /suppliers/{smVendorId}/compliances	This endpoint deletes or replaces compliance data for a single supplier. To delete the existing compliance data for a specified supplier, send an empty response body. To replace all of the existing compliance data for a specified supplier, send the replacement data in the response body.

Prerequisites

- To create an application and request access to use this API, you must have access to the SAP Ariba Developer Portal. For details refer to [Steps to Start Using the SAP Ariba APIs](#) in [Help for the SAP Ariba Developer Portal](#).
- All queries made to this API must be authenticated using OAuth authentication. For details refer to [SAP Ariba Developer Portal Authentication](#) in [Help for the SAP Ariba Developer Portal](#).
- Before adding compliance data to your SAP Ariba Supplier Risk configuration, you must determine the SM Vendor IDs of all relevant suppliers.
- Best practice is to create a new draft version in the SAP Ariba Supplier Risk configuration interface before executing your API updates. For details see [Setting Values and Risk Exposures for Fields](#) in [Setting Up SAP Ariba Supplier Risk](#).
- Best practice is to use the Risk Category Information API for Supplier Risk Exposure with the ARI-13242: Risk exposure override feature.

Restrictions

The manual CSV upload process can't be used to import compliance data.

This API can be used to update compliance data for only one supplier per request. You can bring in any number of evidences for a supplier, but only 100 evidences per API call.

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.

Workflow for Compliance Data in the Risk Category Information API for Supplier Risk Exposure

Use the Risk Category Information API for Supplier Risk Exposure to add compliance data to the supported risk categories for existing suppliers.

1. If not already done, a customer administrator or a member of the **Supplier Risk Manager** group creates a new active version of your risk exposure configuration to verify you have the sanction and watchlist fields. Indicate the weight each field will have on calculation of that supplier's risk exposure. For details see [Setting Values and Risk Exposures for Fields](#) in [Setting Up SAP Ariba Supplier Risk](#).
2. The customer identifies the SM Vendor ID for each desired supplier. This is used to map suppliers to their compliance data. See the Supplier Data API With Pagination in the SAP Ariba Developer Portal.
3. The client application or a customer developer constructs a JSON request body that provides the compliance data for each supplier, identified by SM Vendor ID.
4. The client application passes this JSON to the API to update the SAP Ariba Supplier Risk risk configuration compliance data.

Updating Supplier Compliance Data Using the Risk Category Information API for Supplier Risk Exposure

Use these steps to add, replace, or remove external sanction and watchlist compliance data from the existing suppliers in your risk solution.

Prerequisites

- Best practice is to create a new active version of your risk exposure configuration to verify you have the sanction and watchlist fields. Indicate the weight each field will have on calculation of that supplier's risk exposure. For details see [Setting Values and Risk Exposures for Fields](#) in [Setting Up SAP Ariba Supplier Risk](#).

- Best practice is to use the Risk Category Information API for Supplier Risk Exposure with the ARI-13242: Risk exposure override feature.
- For each supplier, determine the SM Vendor ID. See the Supplier Data API With Pagination in the SAP Ariba Developer Portal.

To export a list of the suppliers and SM Vendor IDs, do the following:

1. 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**.
2. Click **Data import or export**.
3. 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**.
4. Click **Export** to generate a CSV file. You can find the SM vendor ID for each vendor in this file.

Context

Once your SAP Ariba Supplier Risk configuration is complete and you have the SM Vendor ID for the relevant supplier, construct a client application as follows to update the supplier's compliance data in the risk categories:

Note

This API can be used to update compliance data for only one supplier per request.

The manual CSV upload process can't be used to import compliance data.

Note

In the sample URLs in this topic, replace `{{runtime_url}}` with the desired runtime URL from the **Environment Details** table on the SAP Ariba Developer Portal discovery page for this API.

Procedure

1. Construct a JSON query body to update the supplier's compliance data, as follows:

```
{
  "sanctionIndicatorStatus": "VIOLATION_FOUND",
  "watchlistIndicatorStatus": "VIOLATION_NOT_FOUND",
  "supplierScreenedAt": "Jan 01, 2020 00:00:01.001 AM",
  "note": "summary of supplier",
  "evidences": [
    {
      "uniqueId": "unique_evidence_id_1",
```

```

    "source": "test.org",
    "provider": "providerName",
    "penaltyAmount": 1000.5,
    "isoCurrencyCode": "USD",
    "url": "www.test.org/test/1",
    "effectiveStartDate": "Jan 02, 2020 00:00:01.001 AM",
    "effectiveEndDate": "Mar 01, 2020 00:00:01.001 AM",
    "supportingIndicatorStatus": "SANCTION",
    "note": "Summary on data"
  }
]
}

```

sanctionIndicatorStatus	The status that tells you if a sanction was found for the supplier. Permitted values are: Violation_Found , Violation_Not_Found , Violation_Expired , and Not_Screened .
watchlistIndicatorStatus	The status that tells you if the supplier is on a watchlist. Permitted values are: Violation_Found , Violation_Not_Found , Violation_Expired , and Not_Screened .
supplierScreenedAt	The date you screened the supplier for compliance data.
note	Any note you add when you screen the supplier. You can add a note of up to 3000 characters.
uniqueID	An ID that you provide to uniquely identify the evidence data. This isn't a mandatory field. You only need to provide this ID if you want to have the ability to update it later.
source	The source is the origin of the evidence about the supplier. An example is when there are multiple articles supporting the evidence about the supplier, only the most relevant source is shown. You can use the information in the source to find articles from other sources.

Note

The URL for a source must start with **https://** or **http://**.

provider	The provider of the compliance data for the supplier. Your provider can have evidence data from multiple sources.
penaltyAmount	The currency amount of any penalty applied to the supplier for the violation.
isoCurrencyCode	The ISO 4217 currency code that represents the alphabetic currency for the penaltyAmount .
url	The URL used to provide proof of the evidence. The URL is a clickable link. An example is a link to an article.
effectiveStartDate	The date the compliance violation started.
effectiveEndDate	The date the compliance violation ended.
supportingIndicatorStatus	The fields from the risk configurations such as sanction and watchlist .
note	Any note you add about the evidence of the supplier's violation. You can add a note of up to 3000 characters.

2. The client application does one of the following:

- Add your supplier's compliance data in the supported risk categories by using the PATCH /suppliers/{smVendorId}/compliances endpoint, passing the JSON body constructed earlier:

```
PATCH {{runtime_url}}/suppliers?realm=myRealm
{
  "sanctionIndicatorStatus": "VIOLATION_FOUND",
  "watchlistIndicatorStatus": "VIOLATION_NOT_FOUND",
  "supplierScreenedAt": "Jan 01, 2020 00:00:01.001 AM",
  "note": "summary of supplier",
  "evidences": [
    {
      "uniqueId": "My evidence ID 1",
      "source": "https://www.sourceofarticle",
      "provider": "My Data Provider Company",
      "penaltyAmount": 100,
      "isoCurrencyCode": "USD",
      "url": "www.evidencenewsarticle",
      "effectiveStartDate": "Jan 02, 2020 00:00:01.001 AM",
      "effectiveEndDate": "Mar 01, 2020 00:00:01.001 AM",
      "supportingIndicatorStatus": "SANCTION",
      "note": "summary on data"
    }
  ]
}
```

If the supplier doesn't already have compliance data, the new data is created. If the supplier already has compliance data, it's updated.

- Delete or replace your supplier's compliance data in supported risk categories by using the PUT /suppliers/{smVendorId}/compliances endpoint, passing the JSON body constructed earlier:

```
PUT {{runtime_url}}/suppliers?realm=myRealm
{
  "sanctionIndicatorStatus": "VIOLATION_NOT_FOUND",
  "watchlistIndicatorStatus": "VIOLATION_FOUND",
  "supplierScreenedAt": "Jan 01, 2020 00:00:01.001 AM",
  "note": "summary of supplier",
  "evidences": [
    {
      "uniqueId": "My evidence ID 1",
      "source": "https://www.sourceofarticle",
      "provider": "My Data Provider Company",
      "penaltyAmount": 100,
      "isoCurrencyCode": "USD",
      "url": "www.evidencenewsarticle",
      "effectiveStartDate": "Jan 02, 2020 00:00:01.001 AM",
      "effectiveEndDate": "Mar 01, 2020 00:00:01.001 AM",
      "supportingIndicatorStatus": "WATCHLIST",
      "note": "summary on data"
    }
  ]
}
```

To delete the existing compliance data for a specified supplier, send an empty response body. To replace existing compliance data for a specified supplier, send the replacement data in the response body.

Results

On success, the response includes a 201 success code. Within SAP Ariba Supplier Risk the compliance data specified in your PATCH /suppliers/{smVendorId}/compliances or PUT /suppliers/{smVendorId}/

compliances request is assigned to the legal risk category. You can view the imported compliance data in the supplier 360° profile.

On failure, the response includes an error message. See [Risk Category Information API for Supplier Risk Exposure Compliance Data Error Messages \[page 16\]](#) for a list of possible errors.

You can view the data on the applicable risk category tab in the supplier 360°profile. See [Regulatory and Legal Information in a Supplier's Profile](#) in [Monitoring Supplier Risk](#) for sanction and watchlist data.

Users automatically receive one daily email notification at 4:00 a.m. EST that summarizes the adverse media alerts, licensed third-party provider evaluation updates, failure updates for third-party provider Dun & Bradstreet licenses, and supplier compliance updates from the Risk Category Information API for Supplier Risk Exposure, for suppliers they follow.

Risk Category Information API for Supplier Risk Exposure Compliance Data Error Messages

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	The apikey passed in the request is not valid.	The API key passed in the query headers does not match the API key in the OAuth token.
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.

Error Code	Message	Description
400	Please check the value of <code>sanctionIndicatorStatus</code> , value should not be null/empty. Accepted values are: <code>VIOLATION_FOUND</code> , <code>VIOLATION_NOT_FOUND</code> , <code>VIOLATION_EXPIRED</code> , <code>NOT_SCREENED</code> .	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 <code>watchlistIndicatorStatus</code> , value should not be null/empty. Accepted values are: <code>VIOLATION_FOUND</code> , <code>VIOLATION_NOT_FOUND</code> , <code>VIOLATION_EXPIRED</code> , <code>NOT_SCREENED</code> .	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 <code>supplierScreenedAt</code> . Required date format is <code>yyyy-MM-dd</code>	Your JSON request body specifies an invalid date format for <code>supplierScreenedAt</code> . The valid date format is <code>yyyy-MM-dd</code> .
400	Invalid <code>effectiveStartDate</code> . Required date format is <code>yyyy-MM-dd</code>	Your JSON request body specifies an invalid date format for <code>effectiveStartDate</code> . The valid date format is <code>yyyy-MM-dd</code> .
400	Invalid <code>effectiveEndDate</code> . Required date format is <code>yyyy-MM-dd</code>	Your JSON request body specifies an invalid date format for <code>effectiveEndDate</code> . The valid date format is <code>yyyy-MM-dd</code> .
400	Realm <code>YYY</code> in the request does not match with realms in the token. Available realms in token are ' <code>AAA,BBB,CCC</code> '	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 <code>YYY</code> 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: <code>x</code> column: <code>y</code>	There's an error in the data of your JSON request body. Correct the data in the line and column location.
400	<code>supplierScreenedAt</code> should not be a future date	Your JSON request body specifies an invalid date for <code>supplierScreenedAt</code> . The date you screened the supplier for compliance data can't be in the future. Change the date and resubmit.
400	Invalid URL parameter. URL should start with <code>http://</code> or <code>https://</code>	When using PATCH or PUT , the URL for a source must start with <code>https://</code> or <code>http://</code> .
400	Invalid parameter <code>smVendorId</code>	The query URL has an incorrect <code>smVendorId</code> . Correct the SM Vendor ID and resubmit your request.

Error Code	Message	Description
429	Rate limit error	You have exceeded the maximum permitted query rate. Refer to the developer portal discovery page for this API for the applicable query rates.
500	Error deleting compliance data	Resubmit your request later.
500	Error inserting compliance data	Resubmit your request later.
504	Gateway Time-out	The server timeout time has been exceeded, possibly due to network traffic or reliability issues. Retry your query.

Version History for the Risk Category Information API for Supplier Risk Exposure

Please use the active version of the Risk Category Information API for Supplier Risk Exposure.

API Version	Status	As of Release
v1	Active	SAP Ariba 2102
v1	Deprecated the Risk Category Information API	SAP Ariba 2102

ⓘ Note

Starting with release SAP Ariba 2102, the Risk Category Information API was renamed the Risk Category Information API for Supplier Risk Exposure.

Related Information

[Help for the SAP Ariba Developer Portal](#)

[API Versioning and Deprecation on the SAP Ariba Developer Portal](#)

API-Specific Disclaimers and Legal Information

The SAP Ariba Developer Portal included in the SAP Ariba APIs product and the APIs made available on this site are provided solely at the discretion of SAP without warranty of any kind, and SAP may change, suspend, or cancel any or all features or functions of the SAP Ariba APIs product or revise the website at any time. Any production use of or commercialization of applications containing any APIs provided on this website is prohibited without a written agreement between your company and SAP governing such activities.

Access to this API is available to you as a subscriber to this solution as part of the SAP Cloud Service Level Agreement. However, it is not considered part of the solution. Use of this API is purely optional and is subject to restrictions stated in the documentation, including the Terms of Use and the documentation found at the SAP Ariba Developer Portal (see <https://developer.ariba.com/api>). If you wish to connect a third-party service using this API, first confirm that the company is participating in the SAP partner program and is authorized to provide a connection to this solution using this API. You will be required to submit written consent to SAP to authorize the exchange of data with the third-party service.

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.

About the icons:

- Links with the icon  : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
 - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
 - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon  : You are leaving the documentation for that particular SAP product or service and are entering an SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.

The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Bias-Free Language

SAP supports a culture of diversity and inclusion. Whenever possible, we use unbiased language in our documentation to refer to people of all cultures, ethnicities, genders, and abilities.

Copyright © 2026 Ariba, Inc. All rights reserved.

This documentation, as well as the Ariba solutions, software and/or services described in it, contain proprietary information. They are provided under a license or other agreement containing restrictions on use and disclosure and are also protected by copyright, patent and/or other intellectual property laws. Except as permitted by such agreement, no part of the document may be reproduced or transmitted in any form by any means, electronic, mechanical or otherwise, without the prior written permission of Ariba, Inc.

Ariba, Inc. assumes no responsibility or liability for any errors or inaccuracies that may appear in the documentation. The information contained in the documentation is subject to change without notice.

Ariba and Ariba products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of Ariba, Inc. in the United States and other countries. Please see <http://www.ariba.com/legal/trademarks> for additional trademark information and notices.

Ariba Sourcing solutions (On Demand and software) are protected by one or more of the following patents, including without limitation: U.S. Patent Nos. 6,199,050; 6,216,114; 6,223,167; 6,230,146; 6,230,147; 6,285,989; 6,408,283; 6,499,018; 6,564,192; 6,871,191; 6,952,682; 7,010,511; 7,072,061; 7,130,815; 7,146,331; 7,152,043; 7,225,152; 7,277,878; 7,249,085; 7,283,979; 7,283,980; 7,296,001; 7,346,574; 7,383,206; 7,395,238; 7,401,035; 7,407,035; 7,444,299; 7,483,852; 7,499,876; 7,536,362; 7,558,746; 7,558,752; 7,571,137; 7,599,878; 7,634,439; 7,657,461; 7,693,747; 8,364,577; and 8,392,317. Patents pending.

Other Ariba product solutions are protected by one or more of the following patents:

U.S. Patent Nos. 6,199,050, 6,216,114, 6,223,167, 6,230,146, 6,230,147, 6,285,989, 6,408,283, 6,499,018, 6,564,192, 6,584,451, 6,606,603, 6,714,939, 6,871,191, 6,952,682, 7,010,511, 7,047,318, 7,072,061, 7,084,998; 7,117,165; 7,225,145; 7,324,936; 7,536,362; 8,364,577; and 8,392,317. Patents pending.

Certain Ariba products may include third party software or other intellectual property licensed from a third party. For information regarding software or other intellectual property licensed from a third party, go to <http://www.ariba.com/copyrights.cfm>.

