



SAP Ariba 

# 機能の概要

## Risk Category Information API for Supplier Risk Exposure

Lisa Gangewere, SAP Ariba  
一般提供予定: 2021 年 2 月

CONFIDENTIAL

# 機能の概要

導入の難易度 ● ハイタッチ  
対象エリア ● グローバル

## 説明: Risk Category Information API for Supplier Risk Exposure

### 今までの課題

リスクコンプライアンス違反の追跡および警告は、SAP Ariba Risk プラットフォームの柱です。現在、SAP Ariba Supplier Risk では、単一のサードパーティ認可プロバイダとの連携を通じて、監視および制裁措置に関するスクリーニングデータを取り込めるようになっていました。

ただし複雑な組織では、より多くのデータソースオブションが必要となります。また、コンプライアンス担当者は、何らかのコンプライアンス違反があった場合にサプライヤに対して直ちに高リスクとしてフラグが設定される機能を必要としています。

### 対象ソリューション

SAP Ariba Supplier Risk  
SAP Ariba APIs  
SAP Ariba Developer Portal

### SAP Ariba で問題解決

新しい外部 API により、自社開発システムや任意のコンプライアンスパートナーからのコンプライアンス関連情報 (制裁措置および監視に関するスクリーニング結果など) を、裏付けとなる証拠とともに、Ariba Supplier Risk に取り込むことができます。

リスク設定の標準フィールドとして、[制裁措置] フィールドと [監視] フィールドが導入されています。違反は、通常の設定として、リスク影響度計算に対して加重 [高] で設定されます。サプライヤに対してスクリーニングが行われ、制裁措置または監視関連の違反が見つかった場合、全体的な影響度と法規制に関する影響度が [高] (100) となるように設定することができます。

この API で取り込まれた制裁措置および監視に関するスクリーニング情報は、サプライヤプロファイル内の新しい [規制および法] タブに表示されます。

### 関連情報

この機能は、該当するソリューションを導入しているすべてのお客様に対して自動的に有効化されており、すぐに使用できるようになっています。

### 主なメリット

外部 API を使用して SAP Ariba Risk アプリケーションにさまざまなデータソースを含めることができるようになったため、標準/追加の認可サプライヤやカスタムフィールドからデータを取得することもできるようになります。

制裁措置および監視に関する違反が標準フィールドになりました。これらのフィールドは、リスク影響度に寄与し、法および規制に関するリスクカテゴリにマッピングされます。

通常の設定では、制裁措置および監視に関する違反は、[影響度の上書き] フィールドの設定によってリスク影響度に反映され、高リスク (100) に設定されます (ARI-13242 を参照してください)。

サプライヤプロファイル内の新しい [規制および法] タブに、コンプライアンス情報が表示されるようになりました。

### 前提条件と制限事項

この機能を使用するには、SAP Ariba Supplier Risk のライセンスが必要です。

# 機能の概要

## 説明: Risk Category Information API for Supplier Risk Exposure

社内実装チームは、以下の 3 つのタスクを実行し、この機能を有効化します。

### 手順 1: リスク設定:

- サプライヤリスクマネージャは、リスク設定ツールの新しいドラフトを作成して有効化する必要があります。これにより、新しいフィールド [制裁措置]、[監視]、および [影響度の上書き] が表示されます。[制裁措置] フィールドおよび [監視] フィールドには、通常の設定で、[影響度の上書き] フィールドが設定されます。この有効化の処理は、Risk Category Information API for Supplier Risk Exposure を使用してサプライヤレベルのデータを送信する前に完了しておく必要があります。
- 制裁措置および監視の [加重] フィールドは、通常の設定で [高] に設定されています。
- 影響度の上書き (ARI-13242 を参照) を使用する場合、対応するリスクカテゴリがリスク影響度に寄与している必要があります。カテゴリの加重は、1% 以上に設定されている必要があります。

### 手順 2: Risk Category Information API for Supplier Risk Exposure の設定:

- Developer Portal (<https://developer.ariba.com/api/>) にログインし、この API にアクセスします。ユーザーは、ログイン手順に従って、既存のアカウントにログインするか、新しいアカウントを作成することができます。
- SM ベンダ ID は、Risk Category Information API for Supplier Risk Exposure を使用してサプライヤレベルの情報をインポートするために必要な一意の識別子です。顧客はサプライヤの識別に SM ベンダ ID を使用する必要があります。SM ベンダ ID のエクスポートについては、いくつかのオプションが用意されています。
  - Supplier Data API with Pagination を使用して、サプライヤの有効な SM ベンダ ID を取得することができます。
  - [SM 管理] 領域から手動で CSV エクスポート処理を行うと、サプライヤとそれぞれの SM ベンダ ID を識別するためのファイルが作成されます。
  - SLP を使用している場合は、[管理] -> [サプライヤデータのスナップショット] を使用して、すべてのベンダ ID を含むオンボーディングレポートをダウンロードすることもできます。
- Risk Category Information API for Supplier Risk Exposure で送信する情報に、個人情報 (個人用の電話番号など) や機密性の高い個人情報 (生年月日、個人に割り当てられている行政上の ID や金融機関口座番号など) を含めることはできません。送信できるのは公開されているビジネス情報のみとなります。

### 手順 3: Supplier Risk ユーザーインターフェイスでのデータの表示

- API 経由でインポートされたコンプライアンス情報は、SAP Ariba Risk ユーザーインターフェイスで新しい [規制および法] タブに表示されます。
- 制裁措置や監視に関する違反は要因として設定され、サプライヤプロファイルの [リスク影響度] タブに一覧表示されます。
- 制裁措置や監視に関する違反がある場合、リスク影響度の通常設定に基づいて、違反のあったサプライヤに対するリスク影響度が影響度 [高] (100) に設定されます。

## 手順 1: リスク影響度の設定

# 機能の概要

## 説明: Risk Category Information API for Supplier Risk Exposure

Field source	Field	Risk category	Field type	Field value	Weight	Threshold order	Less than	Greater than	Exposure override
Standard	Judgement count	Operational	Numeric		Low	Safer to riskier	1	4	None
Supplier risk exposure API	Sanction	Regulatory & l	Text	Violation found	High				None
Supplier risk exposure API	Watchlist	Regulatory & l	Text	Violation found	High				Overall risk exposure

- 新しい影響度機能が導入されています。選択すると、標準の影響度計算が上書きされます。
  - [全体的なリスク影響度] または [リスクカテゴリの影響度] オプションから選択できます。
- 通常の設定では、[制裁措置] および [監視] フィールドの影響度の上書きは [全体的なリスク影響度] に設定されています。
  - [全体的なリスク影響度] では、サプライヤに高リスクの要因がある場合に全体的な影響度とカテゴリの影響度が [高] に設定されます。
  - [リスクカテゴリの影響度] の場合は、カテゴリの影響度のみが [高] に設定されます。

- 最初のステップとして、リスクマネージャがリスク設定ツールのドラフトを新しく作成し、[制裁措置] および [監視] の新しい標準フィールドと、[影響度の上書き] フィールドが表示されるようにする必要があります。
- [制裁措置] フィールドおよび [監視] フィールドは、リスク設定の標準フィールドとして導入されており、[規制および法] リスクカテゴリにマッピングされています。

[加重] が [高] に設定されています。これは、[影響度の上書き] フィールドを選択する場合の必須の設定です。これにより、影響度が [100] に設定されます。

# 機能の概要

## 説明: Risk Category Information API for Supplier Risk Exposure

Supplier risk administration

Reports

Configure risk exposure

Import data

Configure alerts

Customize supplier alerts

Content and service providers

Adverse media feedback center

Preparation for template upgrade

Manage upgrades

Configure periodic reviews

Back Name: ComplianceAPITest12 Save Cancel Activate

Data sources Category weights Field configurations Incident

Standard fields

Field source	Field	Risk category	Field type	Field value	Weight	Threshold order	Less than	Greater than	Exposure override
Standard	Judgement count	Operational	Numeric		Low	Safer to riskier	1	4	None
Supplier risk exposure API	Sanction	Regulatory & l	Text	Violation found	High				Risk category
Supplier risk exposure API	Watchlist	Regulatory & l	Text	Violation found	High				

Respective category weight should be more than zero to override risk exposure calculations.

- 設定が正しくない場合は、リスクマネージャに対し、対応するタブが赤で表示されます。
- リスク設定のバージョンを保存して有効化する前に、エラーを修正する必要があります。

- [影響度の上書き] フィールドを設定する場合は、対応するリスクカテゴリが [カテゴリ加重] タブのリスク影響度に寄与している必要があります。
- [規制および法] カテゴリの場合は、加重を 1% 以上にする必要があります。
- エラーは、標準フィールドの 2 ページ目に表示されていることがあります。この場合、エラーを確認するにはページ 2/2 を表示する必要があります。

# 機能の概要

## 説明: Risk Category Information API for Supplier Risk Exposure

The screenshots illustrate the configuration of risk categories for supplier risk exposure. The top screenshot shows the 'Field : Sanction' dialog box, where the field value is set to 'Violation found' and the risk level is set to 'High'. The bottom screenshot shows the 'Field : Watchlist' dialog box, where the field value is set to 'Violation found' and the risk level is set to 'High'. Both screenshots show a table of standard fields with columns for Field source, Field, and Risk (L-low, M-medium, H-high).

[制裁措置] フィールドと [監視] フィールドは、利用可能な 4 つの値のいずれかに事前設定されています。制裁措置および監視に関する違反は、リスク影響度の唯一の要因であり、通常設定で、リスク影響度に対する影響度が [高] の要因として設定されています。この加重 [高] は、変更できません。

以下に、コンプライアンスに関するスクリーニングについてバイヤーが入力できる 4 つの値を示します。この情報は、サプライヤプロファイルの [規制および法] タブに表示されます。

- **違反あり** - サプライヤに対するスクリーニングが行われ、制裁措置または監視に関する違反が見つかりました。このシナリオの場合、通常設定で加重が [高] に設定され、リスク影響度に反映されます。
- **違反なし** - サプライヤに対するスクリーニングが行われましたが、制裁措置または監視に関する違反は見つかりませんでした。この状況では、リスク影響度に対する影響はありません。
- **サプライヤスクリーニング済み/未検出** - サプライヤに対するスクリーニングが行われましたが、データベースで該当する事業体が見つかりませんでした。この状況では、リスク影響度に対する影響はありません。
- **サプライヤ未スクリーニング** - サプライヤのコンプライアンス違反に関するスクリーニングが実行されていません。この状況では、リスク影響度に対する影響はありません。

# 機能の概要

## 説明: Risk Category Information API for Supplier Risk Exposure

Name: DS\_TEST\_1

and above which a supplier should be considered risky for the field for risk exposure calculations.

(a) Safer to riskier – indicates value below 'less than' has LOW impact and above 'greater than' has HIGH impact and in-between value has medium impact.

(b) Riskier to safer – indicates values below 'less than' has HIGH impact and above 'greater than' has LOW impact and in-between value has medium impact.

It is defaulted to option (a)

- Less than value
- Greater than value
- Exposure override field - When enabled, it overrides the risk exposure calculation and changes the weight of the selected field to High. When a supplier has a contributing factor of High risk for one of these fields, the score will automatically be set to 100.
  - (a) Overall risk exposure – Set High risk exposure for the supplier overall risk exposure and risk category exposure
  - (b) Risk category exposure – Set the risk exposure to High for the risk category.
  - (c) None – Standard risk exposure calculation applies

Please refer to the examples below for the 'less than value and greater than value' fields:

- If the threshold type is saferToRiskier then anything less than 2 is low, between 2 and 4 is medium and above 4 is high.
- If the threshold type is riskierToSafer then anything less than 2 is high, between 2 and 4 is medium and above 4 is low.

**Licensed fields** are defined as those fields that are contributing factors from a licensed 3rd party provider. This information will be available for Compliance and Financial data and only

Cancel

Field source	Field	Threshold order	Less than	Greater than
Standard	Number of lawsuits	safer to ris	0	1
Standard	Country risk score	riskier to s		
Standard	Number of liens	safer to ris	5	7
Standard	Years since bankruptcy	riskier to s	1	7
Standard	UCC filing count	safer to ris	5	10
Financial	MORE score - current	Financial	High	
Financial	MORE credit limit - current	Financial	None	Riskier to s
Financial	MORE probability of default	Financial	None	Safer to ris

- [?] をクリックすると、ヘルプ情報画面が開き、リスク設定のタブに関する情報にアクセスすることができます。
- [オンラインヘルプ情報] セクションの [標準フィールド]、[ライセンス取得済みのフィールド]、および [カスタムフィールド] セクションに、影響度の上書きに関する情報が追加されています。

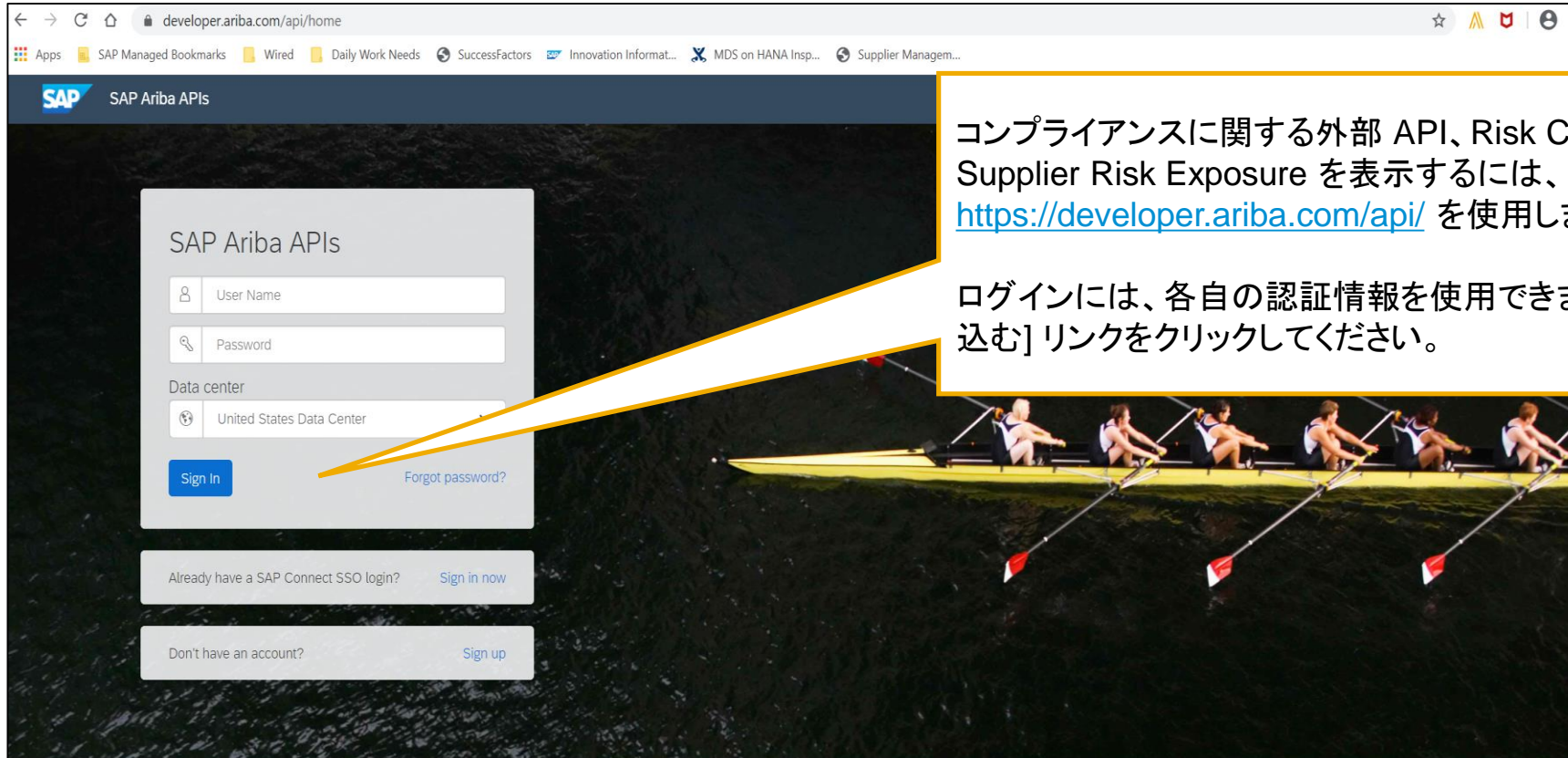


**手順 2:**

**Configure Risk Category Information API for Supplier Risk Exposure – smVendorId の取得**

# 機能の概要

## 説明: Risk Category Information API for Supplier Risk Exposure



コンプライアンスに関する外部 API、Risk Category Information API for Supplier Risk Exposure を表示するには、リンク <https://developer.ariba.com/api/> を使用します。

ログインには、各自の認証情報を使用できます。アカウントがない場合は、[申し込む] リンクをクリックしてください。

Build powerful domain specific applications to address your customer needs using a rich environment and user friendly tools offered by SAP Ariba.

# 機能の概要

## 説明: Risk Category Information API for Supplier Risk Exposure

SAP Ariba APIs- US

Help Lisa Gangewere

ANALYTICS ARIBA NETWORK CATALOG PROCUREMENT STRATEGIC SOURCING **SUPPLIER MANAGEMENT**

REST

- External Approval API for Sourcing and Supplier Management
- Questionnaire Details-Kept for backward compatibility only
- Risk Category Information API
- Supplier Data API
- Supplier Data API With Pagination**

### Supplier Data API With Pagination

Version v4 (Active)

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 Management (new architecture) solution, including supplier names, addresses, registration, qualification, and preferred statuses, and questionnaire details.

For complete documentation of this API, see [Supplier Data API With Pagination](#).

Rate Limit (Requests): 1/second, 100/minute, 4500/hour, 25000/day

#### Release Notes

Supplier Data API With Pagination with OData standards and realm query parameters for auto-enablement support

#### Environment Details

Environment	Description	Value
Sandbox (Mockbox) URL	Sandbox environment with mock sample data. This is not your test or production environment.	<a href="https://openapi.ariba.com/api/supplierdatapagination/v4/sandbox">https://openapi.ariba.com/api/supplierdatapagination/v4/sandbox</a>
Production & Test URL	Runtime URL to access your test and production realm environments.	<a href="https://openapi.ariba.com/api/supplierdatapagination/v4/prod">https://openapi.ariba.com/api/supplierdatapagination/v4/prod</a>
OAuth Server URL Prefix	OAuth Server used by the Cloud Business Applications.	<a href="https://api.ariba.com/">https://api.ariba.com/</a>

Detailed Documentation [Download API Spec](#)

Schemes

**HTTPS**

サインイン後、[Developer (開発者)] 領域 -> [Supplier Management (サプライヤ管理)] に移動すると、利用可能な API を確認できます (画面の左側に表示されています)。

(画面の左側に表示されています。)

# 機能の概要

## 説明: Risk Category Information API for Supplier Risk Exposure

The screenshot shows the SAP API Explorer interface for the 'Supplier Data API With Pagination'. The left sidebar lists various REST APIs, with 'Supplier Data API With Pagination' selected. The main area displays the API details for the POST endpoint '/vendorDataRequests/'. The description states: 'This API will fetch all the vendor details in increments of 500 vendors per page in either JSON or CSV specified in request body. Optionally you can pass on additional filter parameters to get only a subset of vendors. API accepts query param \$skip to get the next page response.' Below the description is a 'Parameters' section with a 'Try it out' button. A table lists the parameters:

Name	Description
request <span style="color: red;">*</span> <span style="color: red;">required</span>	request

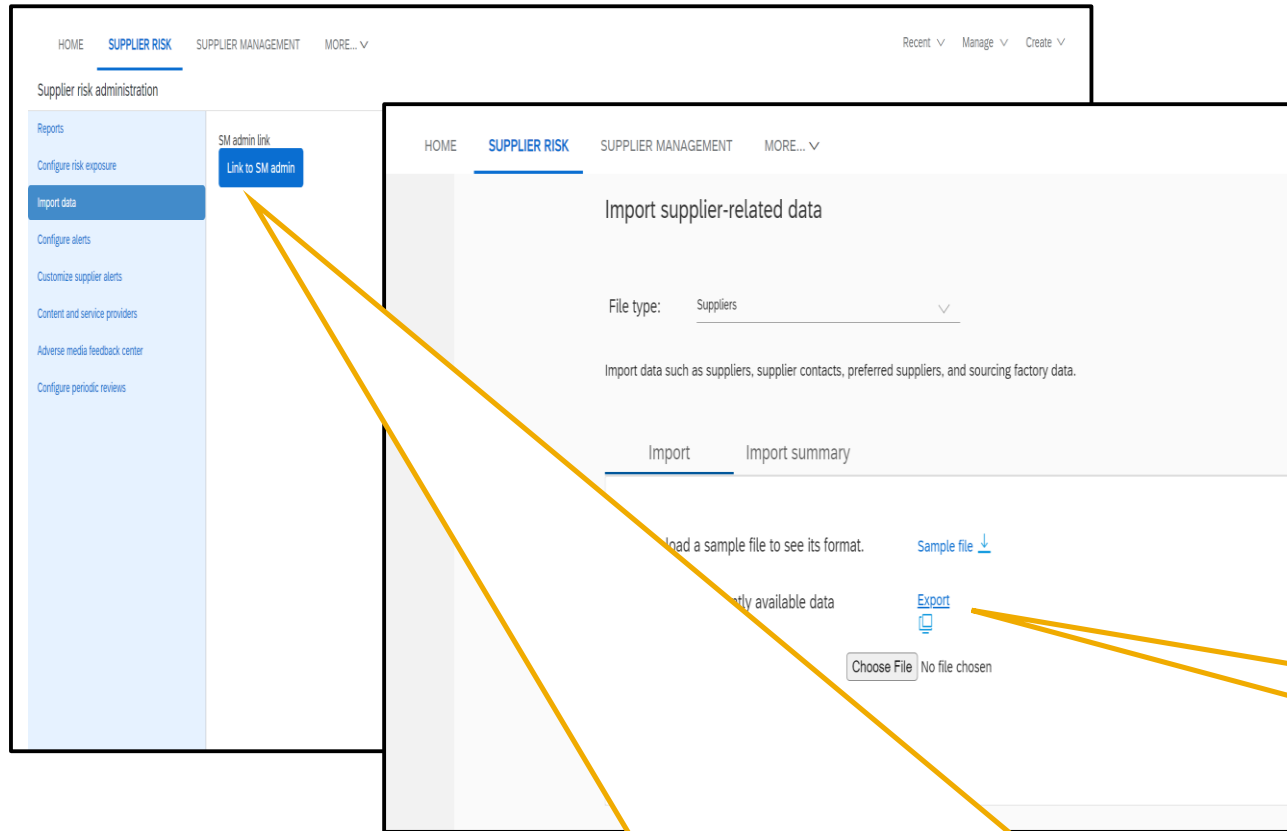
The 'request' parameter is marked as required and has an 'Example Value' link. The example value is a JSON object:

```
{
  "smVendorIds": [
    "string"
  ],
  "businessUnitList": [
    "string"
  ],
  "categoryList": [
    "string"
  ],
  "outputFormat": "CSV",
  "preferredLevelList": [
    0
  ],
  "qualificationStatusList": [
    "Unknown"
  ],
  "regionList": [
    "string"
  ],
  "registrationStatusList": [
    "Unknown"
  ]
}
```

- **Supplier Data API with Pagination:** この API を使用すると、SAP Ariba Supplier Lifecycle and Performance または SAP Ariba Supplier Information and Performance Management (新しいアーキテクチャ) ソリューションから、サプライヤ名、住所、登録、評価、優先状況、質問事項の詳細などのサプライヤデータを取得するクライアントアプリケーションを作成することができます。
- サインイン後、[Developer (開発者)] 領域 -> [Supplier Management (サプライヤ管理)] に移動すると、利用可能な API を確認できます (画面の左側に表示されます)。 Supplier Data API with Pagination が表示されています。
- SM ベンダ ID は、Risk Category Information API for Supplier Risk Exposure を使用してサプライヤレベルの情報を送信するために必要な一意の識別子です。
- サプライヤの SM ベンダ ID を取得するには、Supplier Data API with Pagination を使用します。

# 機能の概要

## 説明: Risk Category Information API for Supplier Risk Exposure



エクスポート CSV ファイルを手動で作成し、自社のレلمムからすべてのサプライヤとそれぞれの SM ベンダ ID をまとめた一覧を取得することもできます。

ダッシュボードから、[SM 管理] に移動します。利用可能なパスは、ユーザーが属するグループによって異なります。

[SM 業務管理者]、[SM ERP 管理者]、または [顧客管理者] グループのメンバは、[SM 管理] を含むサイトで、[管理] -> [SM 管理] を選択できます。

[サプライヤリスクマネージャ] グループのメンバは、SAP Ariba Supplier Risk のダッシュボードから [SM 管理] にアクセスすることができます。

歯車の形をした設定アイコンをクリックしてから、[データのインポート] -> [サプライヤ管理の管理ページ] の順に選択します。

- [エクスポート] をクリックすると、CSV ファイルが生成されます。
- このファイルで、各ベンダの SM ベンダ ID を確認できます。

- [データのインポートまたはエクスポート] をクリックします。
- SLP と SIPM のどちらを使用するかに応じて、[ファイルの種類] プルダウンリストから次のいずれかを選択します。
  - SLP を使用する場合は、[サプライヤ] を選択します。
  - SIPM を使用する場合は、[Sourcing のサプライヤ] を選択します。

## 機能の概要

### 説明: Risk Category Information API for Supplier Risk Exposure

SLP を使用している場合は、[管理] -> [サプライヤデータのスナップショット] を使用して、すべてのベンダ ID を含むオンボーディングレポートをダウンロードすることができます。

[サプライヤデータのスナップショット] レポートに関する詳細については、以下の情報リンクにアクセスしてください。

- サプライヤオンボーディングに関するサプライヤレポートの実行方法:

<https://help.sap.com/viewer/f081c6c38fb7466a84d746a7998bfe0e/cloud/en-US/00736bc3df2944ad9bed8815cb7df76a.html>

- [サプライヤオンボーディングの進行状況] レポート参照:

<https://help.sap.com/viewer/f081c6c38fb7466a84d746a7998bfe0e/LATEST/en-US/cb16676b27f04624b9d6cac0fd588924.html>

手順 2:

**Configure Risk Category Information API for Supplier Risk Exposure – Risk Category Information API へのアクセス**

# 機能の概要

## 説明: Risk Category Information API for Supplier Risk Exposure

Risk Category Information API for Supplier Risk Exposure により、バイヤーは、SAP Ariba Supplier Risk のプロフィールで監視されているサプライヤにサプライヤレベルのデータを追加することができます。

The screenshot shows the SAP Ariba APIs developer portal. The main content area displays the following information:

**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.

For complete documentation of this API, see [Risk Category Information API for Supplier Risk Exposure](#).

Rate Limit (Requests): 5/second, 300/minute, 18000/hour

Release Notes

This is the first version.

Environment Details

Environment	Description	Value
Sandbox (Mockbox) URL	Sandbox environment with mock sample data. This is not your test or production environment.	<a href="https://openapi.qa.cobalt.ariba.com:8443/api/risk-category-information/v1/sandbox">https://openapi.qa.cobalt.ariba.com:8443/api/risk-category-information/v1/sandbox</a>
Production & Test URL	Runtime URL to access your test and production realm environments.	<a href="https://openapi.qa.cobalt.ariba.com:8443/api/risk-category-information/v1/prod">https://openapi.qa.cobalt.ariba.com:8443/api/risk-category-information/v1/prod</a>
OAuth Server URL Prefix	OAuth Server used by the Cloud Business Applications.	<a href="https://svscscdev1mobile.sc1-lab1.ariba.com">https://svscscdev1mobile.sc1-lab1.ariba.com</a>

Detailed Documentation [Download API](#)

Schemes

HTTPS

- サインイン後、[Developer (開発者)] 領域 -> [Supplier Management (サプライヤ管理)] に移動すると、利用可能な API を確認できます (画面の左側に表示されます)。Risk Category Information API for Supplier Risk Exposure が表示されます。

**注:** Risk Category Information API for Supplier Risk Exposure のリリースに伴い、Risk Category Information API は非推奨となります。

API またはバージョンが非推奨となったアプリケーションを使用している場合は、Risk Category Information API for Supplier Risk Exposure のバージョン 1 への移行を開始してください。



# 機能の概要

## 説明: Risk Category Information API for Supplier Risk Exposure

Compliance Data API Compliance Data API allows buyers to add external compliance data to the supported risk categories for existing suppliers in SAP Ariba Supplier Risk

**PATCH** /suppliers/{smVendorId}/compliances Adds compliance data to the supported risk categories for a specified supplier

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.

Parameters Try it out

- この操作を実行すると、単一サプライヤのコンプライアンスデータが追加されます。
- サプライヤにまだコンプライアンスデータがない場合は、新しいデータが登録されます。
- サプライヤにコンプライアンスデータがある場合は、そのデータが更新されます。
- サプライヤデータ (レルム名、smVendorId、コンプライアンスデータ) をインポートする場合は、入力が必要ないいくつかの必須フィールドがあります。

**PUT** /suppliers/{smVendorId}/compliances Replaces compliance data in the supported risk categories for a specified supplier

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

Parameters Try it out

- この操作を実行すると、単一サプライヤのコンプライアンスデータが削除されます。
- 指定したサプライヤの既存のコンプライアンスデータを削除するには、空の要求本文を送信します。
- 指定したサプライヤの既存のコンプライアンスデータを置換するには、応答本文で置換データを送信します。

# 機能の概要

## 説明: Risk Category Information API for Supplier Risk Exposure

Risk Category Information API for Supplier Risk Exposure

Version v1 (Active) ▾

```
ComplianceData {
  sanctionIndicatorStatus string
  example: VIOLATION_FOUND
  Enum:
    Array [ 4 ]
  watchlistIndicatorStatus string
  example: VIOLATION_NOT_FOUND
  Enum:
    Array [ 4 ]
  supplierScreenedAt string
  example: 2020-01-01
  note string
  example: summary of supplier
  evidences [Evidence {
    uniqueId string
    example: unique_evidence_id_1
    source string
    example: test.org
    provider string
    example: providerName
    penaltyAmount integer
    example: 1000.5
    isoCurrencyCode string
    example: USD
    url string
    example: www.test.org/test/1
    effectiveStartDate string
    example: 2020-01-01
    effectiveEndDate string
    example: 2020-05-01
    supportingIndicatorStatus string
    example: SANCTION
    note string
    example: summary on data
  }
  ]
}
```

これは、コンプライアンスデータフィールド定義のフォーマットの例です。

これは、証拠データ定義およびフォーマットの例です。

```
Evidence {
  uniqueId string
  example: unique_evidence_id_1
  source string
  example: test.org
  provider string
  example: providerName
  penaltyAmount integer
  example: 1000.5
  isoCurrencyCode string
  example: USD
  url string
  example: www.test.org/test/1
  effectiveStartDate string
  example: 2020-01-01
  effectiveEndDate string
  example: 2020-05-01
  supportingIndicatorStatus string
  example: SANCTION
  note string
  example: summary on data
}
```

## 機能の概要

# 説明: Risk Category Information API for Supplier Risk Exposure

## 機能の詳細情報

SAP Ariba Developer Portal の使用方法に関するサポートとして、以下のような説明が提供されています。

- ユーザーアカウントを設定し、Developer Portal で使用するアプリケーションを登録する方法
- 利用可能な API を使用するアプリケーションを作成する方法の手順
- OAuth 認証ポータルを組み込む方法

SAP Ariba Developer Portal のヘルプガイドを使用してください。このガイドには、以下のリンクからアクセスできます。

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

# 機能の概要

## 説明: Risk Category Information API for Supplier Risk Exposure

以下は、この API の使用時に表示される可能性のあるエラーメッセージの一覧です。以下の情報は、コンプライアンスデータを更新するために、Risk Category Information API for Supplier Risk Exposure に対するクエリの問題を解決する際に使用します。

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.

**手順 3:**

**Supplier Risk ユーザーインターフェイスでのデータの表示**

# 機能の概要

## 説明: Risk Category Information API for Supplier Risk Exposure

Risk exposure Risk incidents **Regulatory & legal** Enriched corporate info Environmental & social Financial risk

Regulatory & legal  
**High**  
100.0/100.0

Compliance Information

Note	Sanction	Watchlist	Screened Date
summary of supplier	Violation found	Violation found	Feb 23, 2020
summary of supplier	Violation found	Violation found	2020

Evidence

Provider	Source	Note	Penalty amount	Start date	End Date
providerName	test.org	Lorem ipsum dolor sit amet, consectetur ..	USD 1070.5	Mar 7, 2020	Mar 6, 2020
providerName	test.org	ipsum dolor sit amet, consectetur ..	USD	Mar 7, 2020	Mar 6, 2020
providerName	test.org	dolor sit amet, consectetur adipisc ..	USD 1050.5	2020	Mar 6, 2020
providerName	test.org	sit amet, consectetur adipiscing e ..	USD 1040.5	Mar	Mar 6, 2020
providerName	test.org	amet, consectetur adipiscing elit ..	USD 1030.5	Mar 7, 2020	

Risk incidents

Title	Article date	Sub-incident	Source	Language	Feedback reported
<input type="checkbox"/> AWS And Vodafone Focuses On Unlocking Enterprise Opportunity With 5G And Edge Computing	Aug 6, 2020	Corporate Partnership	forbes.com	English	
<input type="checkbox"/> Vodafone's Summer Sale offers up to FIVE times the data on selected plans	Aug 6, 2020	Contracts	thesun.ie	English	

Feedback center Report feedback

- サプライヤプロファイルに、新しい [規制および法] タブが導入されています。
- このタイトルには、バイヤーが Risk Category Information API for Supplier Risk Exposure を使用してサプライヤプロファイルにエクスポートするコンプライアンス証拠情報すべてが含まれます。

- [コンプライアンス情報] 領域には、以下の情報が一覧で表示され、ユーザーが確認できるようになっています。
  - 制裁措置/監視の概要に関するノート
  - 制裁措置の詳細
  - 監視の詳細
  - スクリーニング日 (サプライヤに対してスクリーニングが実行された日の日付スタンプ)
- 時間が経つと、個別のサプライヤに対して提供された情報の履歴にユーザーがアクセスできるようになります。

- このリスク影響度は、[規制および法] カテゴリの影響度を表します
- この例では、サプライヤに制裁措置があり、影響度の上書きに関するフィールドが通常設定として設定されているため、影響度が [高] となっています。

# 機能の概要

## 説明: Risk Category Information API for Supplier Risk Exposure

Risk exposure Risk incidents **Regulatory & legal** Enriched corporate info Environmental & social Financial risk

Regulatory & legal  
**High**  
100.0/100.0

Compliance Information

Note	Sanction	Watchlist	Screened Date
summary of supplier	Violation found	Violation not found	
summary of supplier	Violation found		

Evidence

Provider	Source	Note	Type	Penalty amount	Start date	End Date
providerName	test.org	Lorem ipsum dolor sit amet, consectetur ..	Sanction	USD 1070.5	Mar 7, 2020	Mar 6, 2020
providerName	test.org	ipsum dolor sit amet, consectetur ..	Sanction	USD 1060.5	Mar 7, 2020	Mar 6, 2020
providerName	test.org	dolor sit amet, consectetur adipiscing ..	Sanction	USD 1050.5	Mar 7, 2020	Mar 6, 2020
providerName	test.org	sit amet, consectetur adipiscing e ..	Sanction	USD 1040.5	Mar 7, 2020	Mar 6, 2020
providerName	test.org	amet, consectetur adipiscing elit ..	Sanction	USD 1030.5	Mar 7, 2020	Mar 6, 2020

First < > Last Viewing: 1/2

Risk incidents

Title	Article date	Sub-incident			
<input type="checkbox"/> AWS And Vodafone Focuses On Unlocking Enterprise Opportunity With 5G And Edge Computing	Aug 6, 2020	Corporate Partnership	forbes.com	English	
<input type="checkbox"/> Vodafone's Summer Sale offers up to FIVE times the data on selected plans	Aug 6, 2020	Contracts	thesun.ie	English	

Feedback center Report feedback

このタブの [証拠] セクションには、該当するサプライヤの制裁措置/監視を裏付ける詳細がまとめられ、参照用として表示されます。

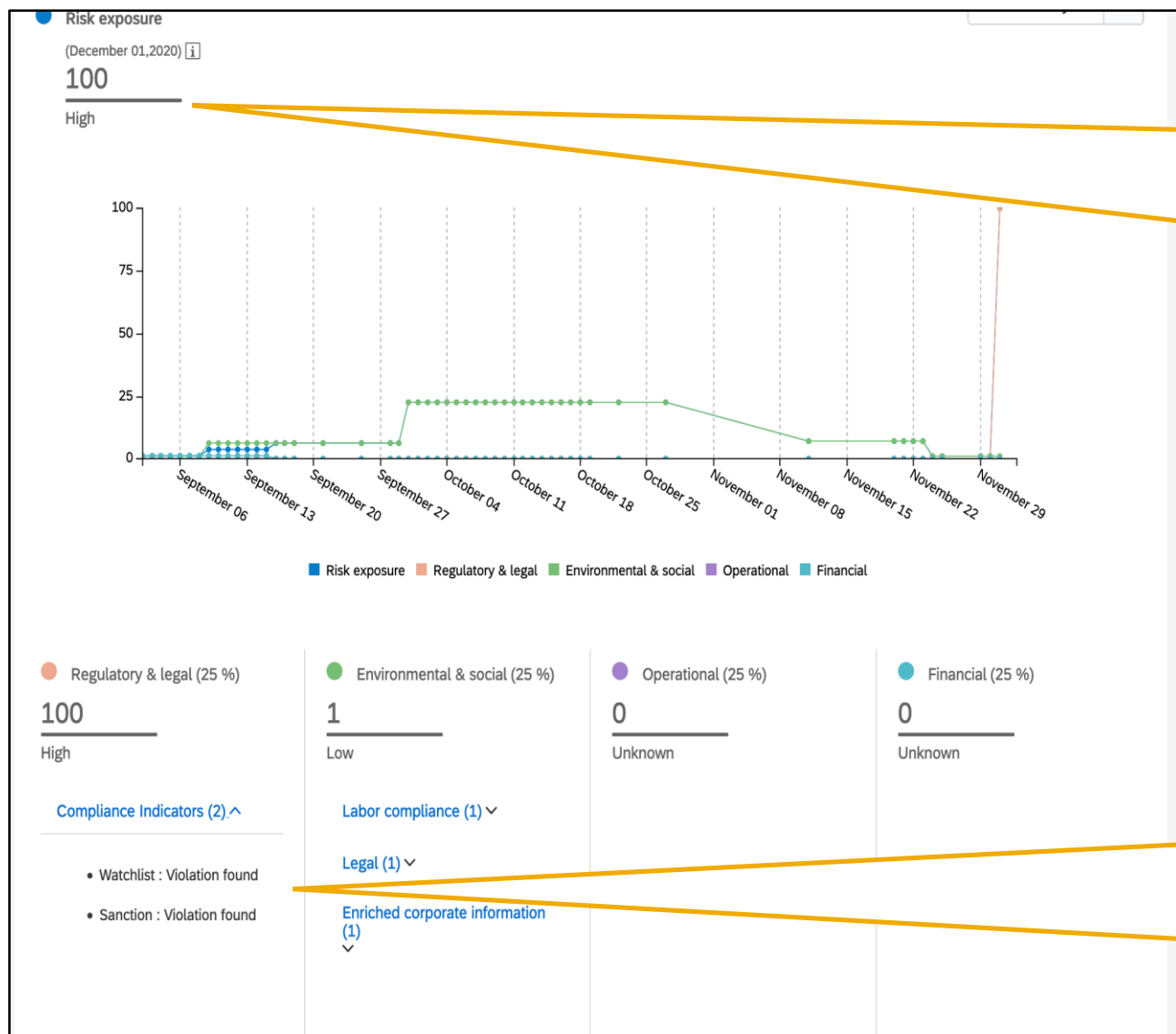
このデータは必須ではないため、バイヤーが情報を入力していない場合、このセクションは空白で表示されることがあります。

- プロバイダ - 制裁措置/監視のソース
- URL - http:// または https:// で始まるリンク
- ノート - これは自由形式のフィールドです。表示される文字数は 25 文字です。マウスのポインタを合わせると、ポップアップで追加情報を確認することができます。
- 開始日 - 違反が始まった日付 (可能であれば)
- 終了日 - 違反が終了した日付 (可能であれば)

[リスクインシデント] セクションには、[規制および法] リスクカテゴリにマッピングされている否定的な情報が含まれます。これらは、サプライヤプロファイルの [リスクインシデント] タブに表示されるリスクインシデントと同じものです。

# 機能の概要

## 説明: Risk Category Information API for Supplier Risk Exposure



• この例では、全体的なリスク影響度が [高] (100)、[規制および法] の影響度が [高] (100) に設定されています。

• このサプライヤーには違反があります。

影響度 [高] が生成され、リスク設定の通常設定が以下のように設定されます。

- 制裁措置 = 加重 [高]
- 監視 = 加重 [高]
- [影響度の上書き] は、通常の設定では [全体的なリスク影響度] に設定されています。

• 制裁措置または監視に関する違反は、現在はリスク設定に標準フィールドとして含まれているため、これらの違反は要因となります。

• サプライヤーに対するスクリーニングが実行されて違反が見つかった場合は、制裁措置または監視に関する違反が [法および規制] リスクカテゴリに対する要因として一覧表示されます。

• [コンプライアンス指標] ラベルをクリックすると、サプライヤープロファイルの新しい [規制および法] タブが開き、バイヤーが裏付けとして提供した証拠を確認できます。



# 機能の概要

## 説明: 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

- リスクカテゴリ情報が更新されたサプライヤをフォローしている Supplier Risk ユーザーには、そのサプライヤが Risk Category Information API for Supplier Risk Exposure からのデータを使用して更新されたことを示す情報が、日次電子メール通知で届きます。

# 機能の概要

## 説明: 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.  
© 2020 SAP SE. All rights reserved

- リスクカテゴリ情報が更新されたサプライヤをフォローしている Supplier Risk ユーザーには、そのサプライヤが Risk Category Information API for Supplier Risk Exposure からのデータを使用して更新されたことを示す情報が、日次電子メール通知で届きます。

# 機能の概要

## 説明: Risk Category Information API for Supplier Risk Exposure

### 機能の詳細情報と最良事例

- 最初のステップとして、リスクマネージャの権限を保有している Supplier Risk ユーザーが、リスク設定ツールの新しいドラフトを作成する必要があります。[影響度の上書き] フィールドに対して既定の通常設定を使用している場合は、これにより、標準フィールド [制裁措置]、[監視]、および [影響度の上書き] が表示されるようになります。この処理は、Risk Category Information API for Supplier Risk Exposure を使用してサプライヤレベルのデータをインポートする前に完了しておく必要があります。
- 制裁措置および監視の [加重] フィールドは、通常の設定で [高] に設定されていますが、設定を変更することもできます。
- 標準フィールド [制裁措置] および [監視] に対しては、通常の設定で [影響度の上書き] フィールドが有効になっており、[全体的な影響度] に設定されています。
- 影響度の上書きを使用する場合、対応するリスクカテゴリがリスク影響度に寄与している必要があるため、このカテゴリの加重は 1% 以上に設定します。
- リスク設定では、標準フィールドが 2 ページにわたっているため、リスク設定の [フィールド設定] タブにエラーがある場合は、2 ページ目を表示してエラーをチェックする必要があります。
- Risk Category Information API for Supplier Risk Exposure にアクセスするには、Developer Portal (<https://developer.ariba.com/api/>) にログインし、この API にアクセスします。
- Risk Category Information API for Supplier Risk Exposure の使用時には、SM ベンダ ID を使用してサプライヤを識別する必要があります。SM ベンダ ID は、サプライヤレベルの情報をインポートする際の一意の識別子となります。
- サプライヤの SM ベンダ ID を取得するには、Supplier Data API with Pagination を使用します。
- [SM 管理] から手動での CSV エクスポート処理を使用して、サプライヤと SM ベンダ ID を識別するためのファイルを作成することもできます。
- Risk Category Information API for Supplier Risk Exposure で送信する情報に、個人情報 (個人用の電話番号など) や機密性の高い個人情報 (生年月日、個人に割り当てられている行政上の ID や金融機関口座番号など) を含めることはできません。送信できるのは公開されているビジネス情報のみとなります。