Sample Document of Implementing VendorVerifier in SAP ARIBA Supplier Risk
Supplier Module in SAP Ariba

Adding VendorVerifier to a Supplier Engagement Request

Unique URL to VendorVerifier: [SAMPLE URL]

1. Go to your templates -> Supplier Risk Engagement Project Template

2. Go to documents -> Inherent Risk Screening Questions
3. Go to the content section in your Inherent Risk Screening Questions

1. Click on the add button

1.a. Click on the add section button.
1.b. Create a section name based on which model you wish to add to your sourcing project
   1.b.i. Mandatory Cybersecurity Policy
   1.b.ii. Optional Use of VendorVerifier to Build Cybersecurity Policies
1. b. iii. Certification for Cybersecurity
   1. b. iv. Remote Working Policy
   1. b. v. Final Attachments

2. Mandatory Cybersecurity Policy
   2.a. Use this option if you want to push cybersecurity compliance towards your supply chain
   2.b. Click the add button
   2.c. Click the requirement in the dropdown

2.d. Copy and Paste the following text into the Requirement field:
We believe that cybersecurity policies are an important aspect of protecting each other’s businesses. To ensure a safe working partnership, we have added a platform that allows you to build policies if you do not have them or assess those that you do. Please click on the link below to create an account and protect your business from cybersecurity threats and attacks.

[SAMPLE URL]

3. Optional Use of VendorVerifier to Build Cybersecurity Policies
   3.a. Use this option if you want to provide a tool to help your suppliers with cybersecurity compliance but leave it as a choice to the supplier to utilize the tool
   3.b. Click the add button
   3.c. Click the question in the dropdown
   3.d. Change Answer Type to: Yes/No
   3.e. Copy and Paste the following text into the Name field:
      We believe that cybersecurity policies are an important aspect of protecting each other’s businesses. To ensure a safe working partnership, we have procured a platform that allows you to build policies if you do not have them or assess those that you do. Would you like to use the platform we’ve procured for you to build and assess your cybersecurity policies?
   3.f. Click the add button
3.g. Click the requirement in the dropdown.

3.h. Copy and Paste the following text into the Requirement field:

Please click on the link below to create an account and protect your business from cybersecurity threats and attacks. [SAMPLE URL]

3.i. Click the dropdown for Visibility Conditions

3.i.i. Click the create conditions.
3.iii. Select the question that you’ve created in step 6.g.

3.iii. Select yes for the expression
3.iii. Click ok

4. Certification for Cybersecurity
   4.a. Use this option if you would only like to provide the VendorVerifier tool for those with no internationally recognized certification for cybersecurity (eg. ISO 27001/27002, IEC, etc.)
   4.b. Click the add button
   4.c. Click the question in the dropdown
   4.d. Change Answer Type to: Yes/No
   4.e. Copy and Paste the following text into the Name field:
   4.f. Do you have an internationally recognized certification for cybersecurity? (examples include: ISO 27001/27002, IEC, etc.)
   4.g. Click the add button
   4.h. Click the question in the dropdown
   4.i. Copy and Paste the following text into the Name field:
   4.j. Attach Certification
   4.k. Change Answer Type to: Attachment
   4.l. Click the dropdown for Visibility Conditions
      4.l.i. Click the create conditions
      4.l.ii. Select the question that you’ve created in step 7.f.
      4.l.iii. Select yes for the expression
      4.l.iv. Click ok
   4.m. Click the add button
   4.n. Click the requirement in the dropdown
   4.o. Copy and Paste the following text into the Requirement field:
   We believe that cybersecurity policies are an important aspect of protecting each other’s businesses. To ensure a safe working partnership, we have added a platform that allows you to
build policies if you do not have them or assess those that you do. Please click on the link below to create an account and protect your business from cybersecurity threats and attacks.

[SAMPLE URL]
4.p.Click the dropdown for Visibility Conditions
   4.p.i.Click the create conditions
   4.p.ii.Select the question that you’ve created in step 7.f.
   4.p.iii.Select no for the expression
   4.p.iv.Click ok

5. Remote Working Policy
5.a.Use this option if you are worried about your supply chain becoming more vulnerable to cyber attacks and theft post pandemic due to their employees working remotely
5.b.Click the add button
5.c.Click the requirement in the dropdown
5.d.Copy and Paste the following text into the Requirement field:
Due to the pandemic and the increased cybersecurity risks associated with remote working, we recommend to all our suppliers to build a Work from Home Policy that will help you manage remote access for your employees. We are providing this service at no cost to you. Please follow the link and steps below to access your NIST Cybersecurity Framework policy templates and assessments.

[SAMPLE URL]

6. Final Attachments

7. Use this option if you wish to see the results of your suppliers policy assessments
7.a.Click the add button
7.b.Click the requirement in the dropdown
7.c.Copy and Paste the following text into the Requirement field:
Once you’ve completed all the VendorVerified policies, please attach the Document Relevance Dashboard export.
7.d.Click the add button
7.e.Click the Question in the dropdown
7.f.Change Answer type to: Attachment
7.g.Copy and Paste the following text into the Requirement field:
Please attach the Document Relevance Dashboard export.

8. Add additional content as needed

9. Review in summary

10. Publish the Inherent Risk Screening Questions

11. Go back to the home screen -> Create -> Engagement Request