



# 供应商入职 Ariba 用户指南

## 第三方风险管理

### 风险评估

对于供应商

## 风险控制评估 - 它是什么？



对于与 IPG 开展业务的新供应商，可能会触发五种风险控制评估。

**1. 合规性；2. 腐败；3. 现代奴隶制；4. 隐私；5. 信息安全**

## 设置上下文



根据 IPG 的前期控制和检查，IPG 可能会向供应商发送风险控制评估，以进一步评估 IPG 与新供应商开展业务时的风险敞口。供应商可能会收到一 (1) 至五 (5) 项要答复的风险控制评估。

## 主要优点

1. 风险控制评估通过 Ariba 门户直接发送给供应商。**需要答复风险控制评估。**
2. 供应商可以利用其现有的 Ariba Network 帐户
3. 风险控制评估是动态的——**只有适用的**评估才会发送给供应商

## 流程



机构请求者



供应商



供应商风险管理团队

启动风险评估流程。发送风险问卷给供应商

提供所需风险控制评估的答复和文件

审查已完成的风险控制评估并确定控制措施是否有效或无效

1. 供应商可能会收到额外的电子邮件通知，要求他们提交符合 **IPG 供应商风险评估流程** 的风险控制问卷。点击电子邮件中的链接。
2. 供应商将使用其现有凭证登录 Ariba SLP。此链接将自动带供应商到选定的问卷。需要答复风险控制问卷。

Action needed: Complete questionnaire from [US17] - FutureBrand New York



To <s4system-prod3+ipg-T.Doc235435812@ansmtp.ariba.com>  
● 供应商联系方式

Reply Reply All Forward ...



Hello 供应商联系方式,

[US17-US84] - FutureBrand New York has invited you to complete a questionnaire. This is required so Big Red Dog Production LLC can do business with [US17-US84] - FutureBrand New York.

**Questionnaire Overview**

Questionnaire name: Security  
Respond by: Sat, 11 Sep, 2021  
Update Request Comments:

[Submit questionnaire](#)

Best,  
[US17-US84] - FutureBrand New York

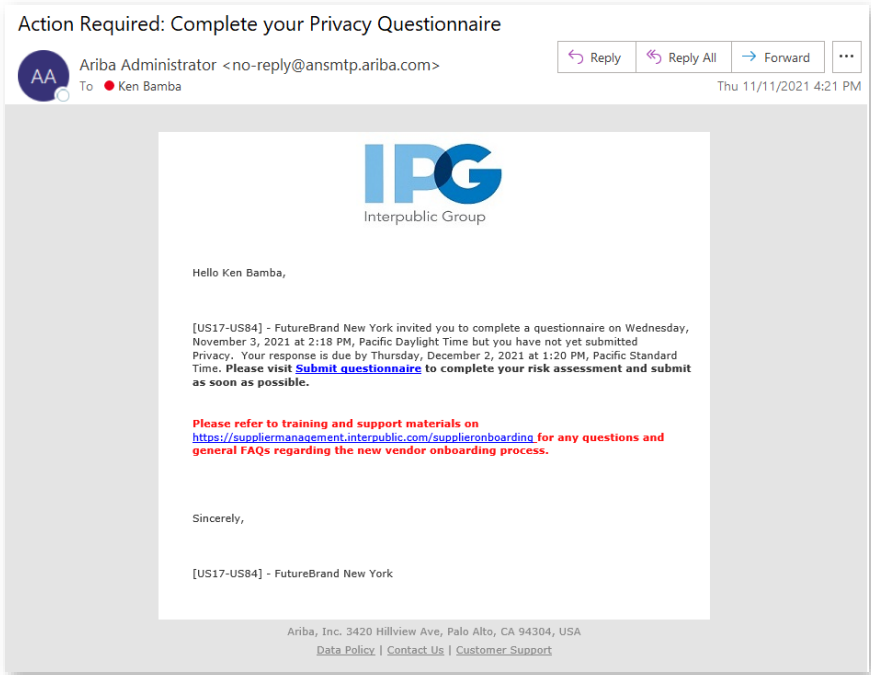
Ariba, Inc. 3420 Hillview Ave, Palo Alto, CA 94304, USA  
[Data Policy](#) | [Contact Us](#) | [Customer Support](#)

# 完成并提交风险控制评估

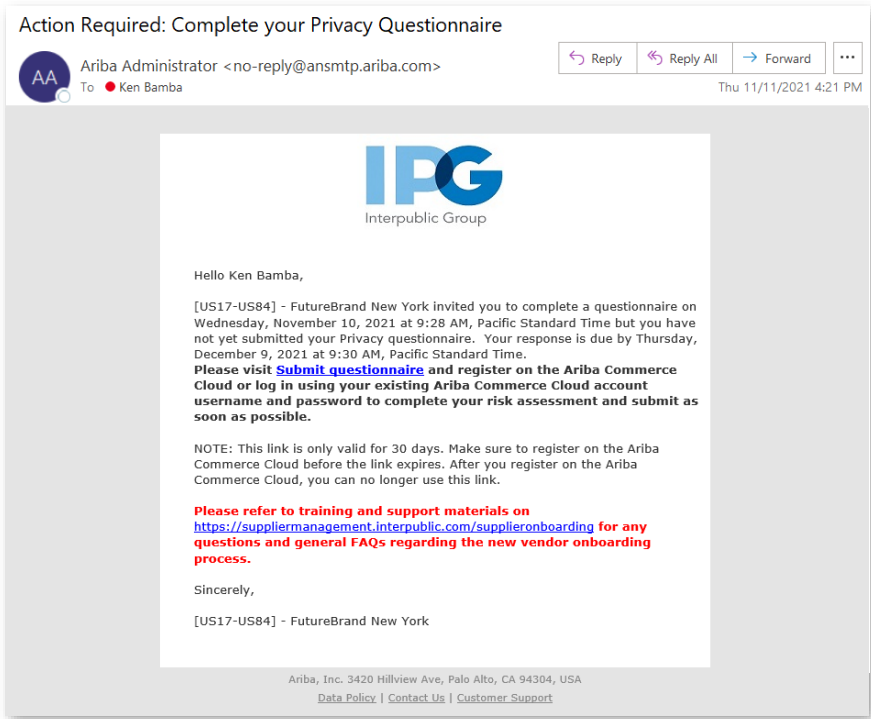
如果供应商在初始电子邮件通知提示时未立即完成风险控制评估，他们将在 30 天内每 5 天收到一封提醒电子邮件通知，要求他们提交符合 IPG 供应商风险评估流程的风险控制问卷。

电子邮件的形式如下：

每次触发风险控制评估都会收到：



如果供应商没有 Ariba 帐户，则触发每次风险控制评估时都会收到：



# 完成并提交风险控制评估

**指定的风险控制问卷** 将提示供应商回答五个风险领域之一的问题：合规、腐败、现代奴隶制、隐私或信息安全。**需要答复风险控制问卷。**

1. 完成 指定的风险控制问卷。提供答案并选择这些标准是否适用。

• 如果需要， 供应商可以向任何带有图标的问题添加评论和附件。

- 在评论章节输入评论。
- 单击“附加文件”可将附件添加到问卷中。
- 单击“确定”保存评论。供应商将返回到问卷，添加评论和附件的图标将如下所示：



# 完成并提交风险控制评估

**风险控制评估** 是动态的——供应商对某些问题的回答可能会改变这些必答题。一旦供应商对所有必答题和条件题做出了答复：

- 2. 点击 **提交全部答复**，以提交风险控制问卷。**保存草稿**，以便稍后完成风险控制评估。**请注意，为了让 IPG 看到答复，必须单击“提交整个答复”。**
- 3. 单击 **确定** 提交评估。这将通知 IPG 的风险团队风险控制评估已完成。

All Content

Name ↑

65	Are disaster recovery and response plans tested?	<div>Yes</div>
66	In the event of a disaster, is there an Recovery Time Objective defined for this service? If Yes, please provide the intended recovery time in the comments section	<div>Yes</div>
67	Is this a global policy?	<div>Yes</div>
68	Are restore procedures periodically tested to verify that data being backed up is usable?	<div>Yes</div>
69	Do you have Cyber insurance?	<div>Yes</div>
70	If yes, does coverage include first and third parties?	<div>First Party Only</div>
71	What is your liability coverage?	<div>Greater or equal to 5 million</div>
72	Do you regularly monitor or audit the security controls used by your Third Party Service Providers?	<div>Yes</div>
73	Are third-party external service providers' activity monitored to detect potential cyber security events?	<div>Yes</div>
74	Do third parties undergo a risk assessment/due diligence before services are exchanged?	<div>Yes</div>
75	Are outside parties made aware of the applicable company security policies prior to being granted access to the application and/or the environment?	<div>Yes</div>
76	Please provide your latest Web Application Vulnerability Scan Report for review.	<div>File Attached</div>
77	Please provide a copy of your latest SOC 2 type 2 report for review.	<div>File Attached</div>
78	Please provide a copy of your latest ISO27001 report and certification for review.	<div>File Attached</div>
79	Please provide your latest Network Vulnerability Scan Report for our review.	<div>File Attached</div>
80	Please provide any other certifications you feel may be relevant to the review of your business and services provided. I.E. (FedRamp, SOX, PKI (HIPAA, etc.), PCI DSS, PII (Safe Harbor, etc.), GDPR, CCPA)	<div>File Attached</div>
81	Provide a copy of a data flow diagram for the services your company provides (or is planning to provide) to IPG or its agencies.	<div>File Attached</div>

(\*) Indicates a required field

Submit Entire Response

Save draft

Compose Message

Excel Import

✓

Submit this response?

Click OK to submit.

OK

Cancel

# 完成并提交风险控制评估

提交风险控制评估后，供应商将在页面顶部看到评估已完成的确认栏。

4. 单击“**返回 IPG 仪表板**”，以 返回到 Ariba 提案和问卷仪表板。

Ariba Sourcing

Go back to IPG - TEST Dashboard

Company SettingsKen Bamba

Desktop File Sync

Time remaining  
364 days 23:58:37

Console

Doc235435802 - Security

Event Messages  
Event Details  
Response History  
Response Team

Event Contents

All Content

✓ Your revised response has been submitted. Thank you for participating in the event.

All Content

Name ↑	
1 Are documented Information Security Policies reviewed and updated annually and include at a minimum: <ul style="list-style-type: none"><li>Access Control Policy</li><li>Acceptable Use Policy</li><li>Password Policy/Standard</li><li>Vulnerability Management</li><li>Security Incident Management</li><li>Risk Management</li><li>Business Continuity</li><li>Change Management</li><li>Physical Security</li><li>HR that includes background checks &amp; training data management</li></ul>	Yes
2 Do you clearly define IT security-related roles and responsibilities for your personnel (including the limitation of each role and the level of training required)?	Yes
3 Do you have a Security User Awareness program?	No

Compose Message

- 如果需要对已提交的答复进行编辑，请返回到该文档并选择 **修改答复**，这将重新打开问卷进行编辑。先前的答复将保存在该工具中。

Doc252619553 - HIPAA

Time remaining  
364 days 23:59:34

If your customer has requested an update to this questionnaire, please click **Revise Response** and re-submit your answers. Even if you do not need to change any of your current answers, your customer cannot complete their evaluation until you re-submit the questionnaire.

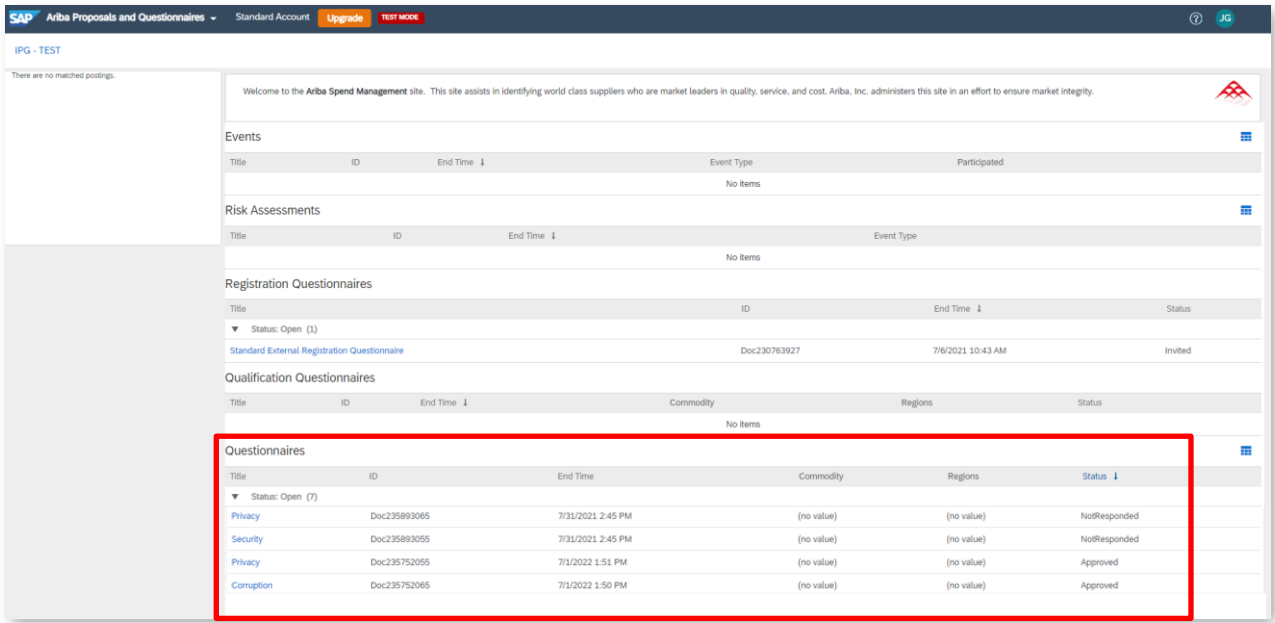
Revise Response

All Content

Name ↑	
1 Do you have an assigned security official responsible for implementing HIPAA/HITECH administrative safeguards?	Yes
2 Have you implemented administrative, technical and physical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of PHI that you Process on behalf of IPG or its agencies?	No
3 Do you ensure that any agents or Third Party Service Providers to whom you provide PHI agree to the same restrictions that we impose on you?	No

**Ariba 提案和问卷仪表板** 为供应商联系人提供了所有已指定文档的概览：

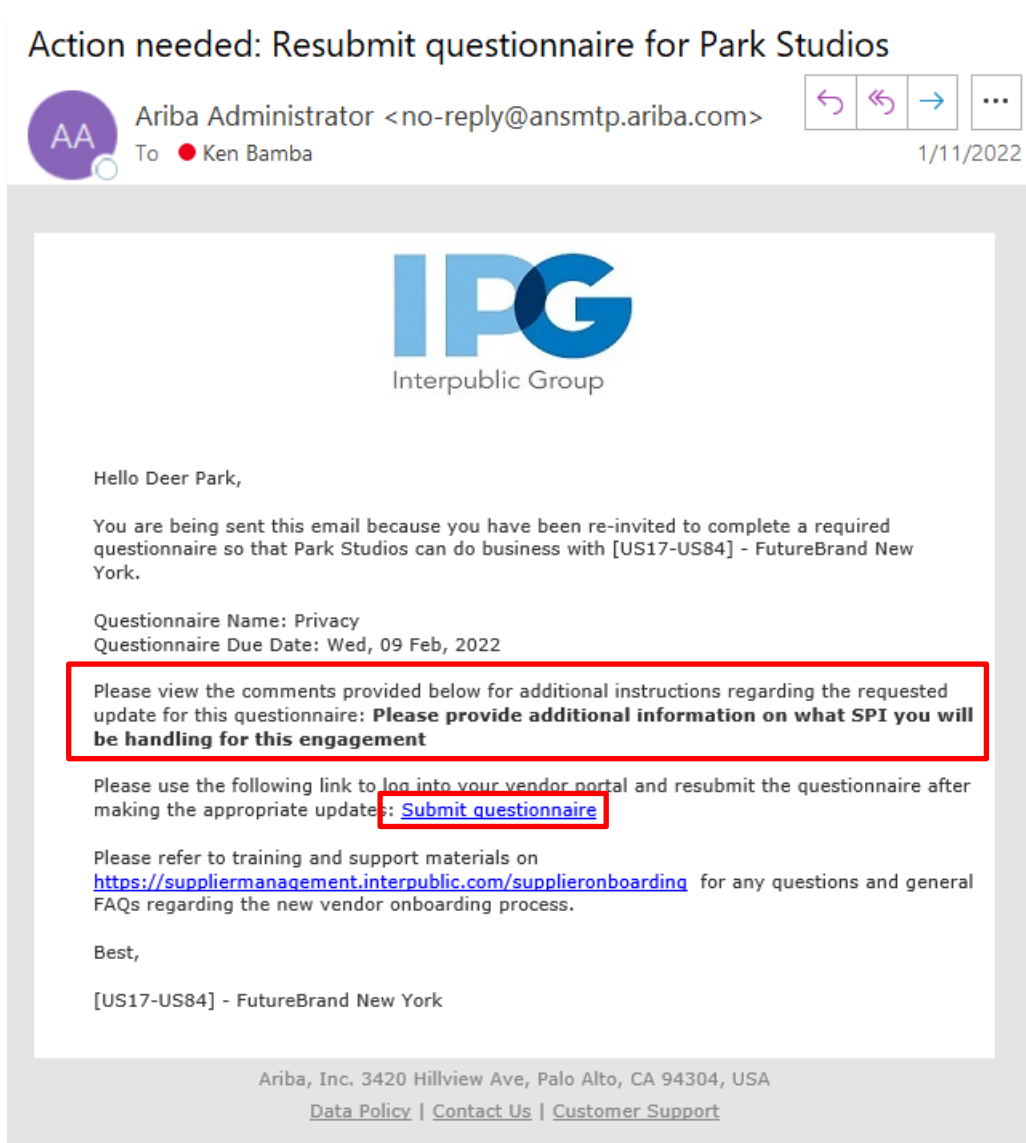
- 活动
- 任务
- 问卷
- 证书



4. 滚动到 **问卷** 选项卡即可查看所有完成和未完成的问卷的列表。
  - 点击风险控制评估的 **标题**，以查看/修改问卷的答复。问卷必须处于“**已批准**”状态才能编辑。供应商还可以填写状态为 **未答复的调查问卷**。
5. 完成所有处于 **未答复** 状态的问卷。



如果需要，IPG 团队可能会根据供应商对问卷的答复 **请求更多信息**。供应商联系人可能会收到一封包含 **更新请求评论** 的电子邮件。



1. 查看评论/IPG 审稿人提出的后续问题。
  2. 点击“**提交问卷**”即可返回问卷。供应商可以修改答复、添加其他评论并添加任何新文档。完成后，提交问卷。
- **注意：** 请注意，IPG 可能会通过电子邮件联系供应商，以解决风险评估过程中发现的任何问题或控制漏洞。