PROJECT RISK ASSESSMENT QUESTIONNAIRE

VENDOR NAME	VENDOR ADDRESS

POINT OF CONTACT	CONTACT INFORMATION

INSTRUCTIONS: Please complete this questionnaire in its entirety, leaving notes and attaching supporting documentation where necessary.

Nature of Data Vendor Will Have Access to *check all that apply*

X	DATA TYPE		NOTES
	No exchange of data		
	Demographic data		
	Financial data		
	Personal data (e.g., name, address, phone number)		
	Non-public personal data (e.g., SSN, medical, proprietary)		
	Other:		

POLICIES AND PROCESSES

Yes	No	N/A	QUESTION	NOTES
			Does your organization document, publish, and enforce security policies?	
			Does your organization document and enforce HR policies?	

			Does your organization document and enforce policies for authorized use of networked services?	

POLICIES AND PROCESSES *continued*

Yes	No	N/A	QUESTION	NOTES
			Does your organization document and enforce policies for authorized use of company email, internet, and intranet?	
			Does your organization document and enforce encryption policies and standards?	
			Does your organization document and enforce policies regarding the storage, use, and disposal of sensitive data?	
			Does your organization document and enforce policies regarding the storage, use, and disposal of sensitive data by third parties?	
			Does your organization outsource functionalities related to security management?	
			Do policies and procedures adhere to and comply with privacy laws and regulations related to the security, concealment, and safeguarding of customer data?	
			Are the penalties associated with non-compliance to your organization’s policies well documented?	
			[Insert Policies and Processes Question Here]	
			[Insert Policies and Processes Question Here]	

			[Insert Policies and Processes Question Here]	

PHYSICAL AND DATA CENTER SECURITY MEASURES

Yes	No	N/A	QUESTION	NOTES
			Does your organization regularly review and assess physical and environmental risks?	
			Do data center perimeter controls involve the use of access cards?	
			Do data center perimeter controls involve the use of keypad controls?	
			Do data center perimeter controls involve the use of security guards?	
			Do data center perimeter controls involve the use of __[add measure here]__?	
			Do you have business continuity procedures in place if the office is inaccessible for any reason?	
			Is all network equipment physically secured?	
			Does your organization use data center providers?	
			Does your organization utilize visitor logs? If so, are they maintained for more than 30 days?	
			Does your organization maintain a written policy regarding physical security requirements for the office?	

			[Insert Physical and Data Center Security Question Here]	
			[Insert Physical and Data Center Security Question Here]	

MALWARE SECURITY MEASURES

Yes	No	N/A	QUESTION	NOTES
			Are all emails scanned for viruses?	
			Is anti-virus software required and enabled on all network computers?	
			Does anti-virus software have an established frequency of scanning on network computers?	
			Does your organization allow the installation of non-approved software on network computers?	
			[Insert Malware Security Question Here]	
			[Insert Malware Security Question Here]	
			[Insert Malware Security Question Here]	

INFORMATION SECURITY MEASURES

Yes	No	N/A	QUESTION	NOTES
			Does your organization have an information security program in place? (In the notes column, please provide a link to all relevant public-facing security and privacy policies.)	
			If your organization has an information security program, does it apply to all operations and systems that process sensitive data?	
			Are relevant staff and managers professionally certified in information security?	
			Is administrator-level access limited on network infrastructure?	
			Are strict controls in place in order to access security logs?	
			[Insert Information Security Question Here]	
			[Insert Information Security Question Here]	
			[Insert Information Security Question Here]	

NETWORK INFRASTRUCTURE SECURITY MEASURES

Yes	No	N/A	QUESTION	NOTES
			Does your organization maintain a network security policy?	
			Are all routers systematized with access control lists to stifle unauthorized traffic?	
			Are server operating systems patched at the latest level?	
			Does your organization have a process in place to track and communicate vulnerability patches?	
			Does your organization back up your data?	
			Are backups stored and tested?	
			Are employee devices encrypted?	
			Is a third party used to test network infrastructure security?	
			Do you employ intrusion detection systems?	
			[Insert Network Infrastructure Security Question Here]	
			[Insert Network Infrastructure Security Question Here]	
			[Insert Network Infrastructure Security Question Here]	

ADDITIONAL INFORMATION

RISK ASSESSOR NAME AND TITLE SIGNATURE DATE

DISCLAIMER

Any articles, templates, or information provided by Smartsheet on the website are for reference only. While we strive to keep the information up to date and correct, we make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability with respect to the website or the information, articles, templates, or related graphics contained on the website. Any reliance you place on such information is therefore strictly at your own risk.