InfoSec Vendor Onboarding Document

Overview: The SVM team has migrated its vendor portfolio to a cloud-based hosted SaaS solution and many of the existing processes have changed, impacting your engagement with the assessment process.

Intended Audience: This document is created for a 3rd party vendor who has an established business relationship with Walgreens and is required to complete an online vendor assessment.

Purpose: The purpose of this document is to support the 3rd party vendor with answering basic questions associated with the dynamic questionnaire process.

Prerequisite: The 3rd party must already have established a Walgreens ID within the MyPassport system. This means that the user has received an initial email from the IDAdmin team and authenticated into the MyPassport Identity System, set their permanent password, and established their secondary MFA (Multi-Factor Authentication) device.

Support: If there are any concerns regarding this document, please contact the IDAdmin team at WBAVendorMgtIdentity@walgreens.com.

TABLE OF CONTENTS

Contents

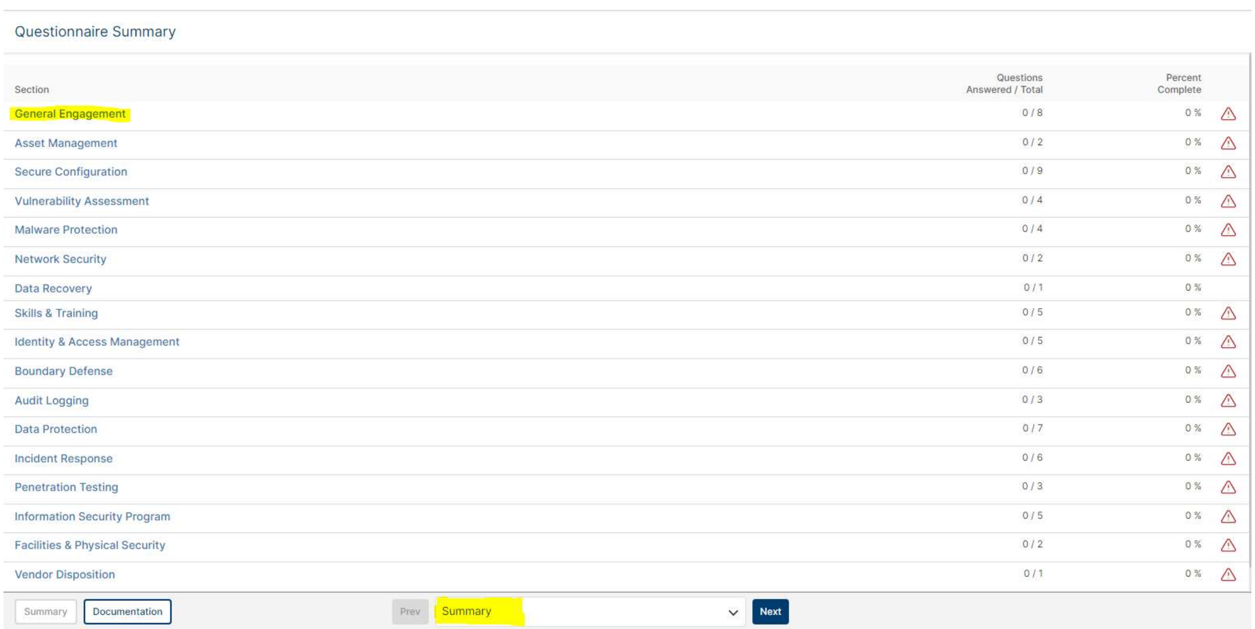
Adding Additional Vendor Contacts

If additional vendor contacts are needed, please use the *dialog* box for response and send the follow details about the new contact back to Identity Admin team at WBAVendorMgtIdentity@walgreens.com

- First Name
- Last Name
- Email Address

Completing the Questionnaire

Upon login to the system, you will see the active questionnaire sections. From this page, you can navigate to the individual questions by clicking on either the “Summary” drop-down at the bottom or the “Section” name:

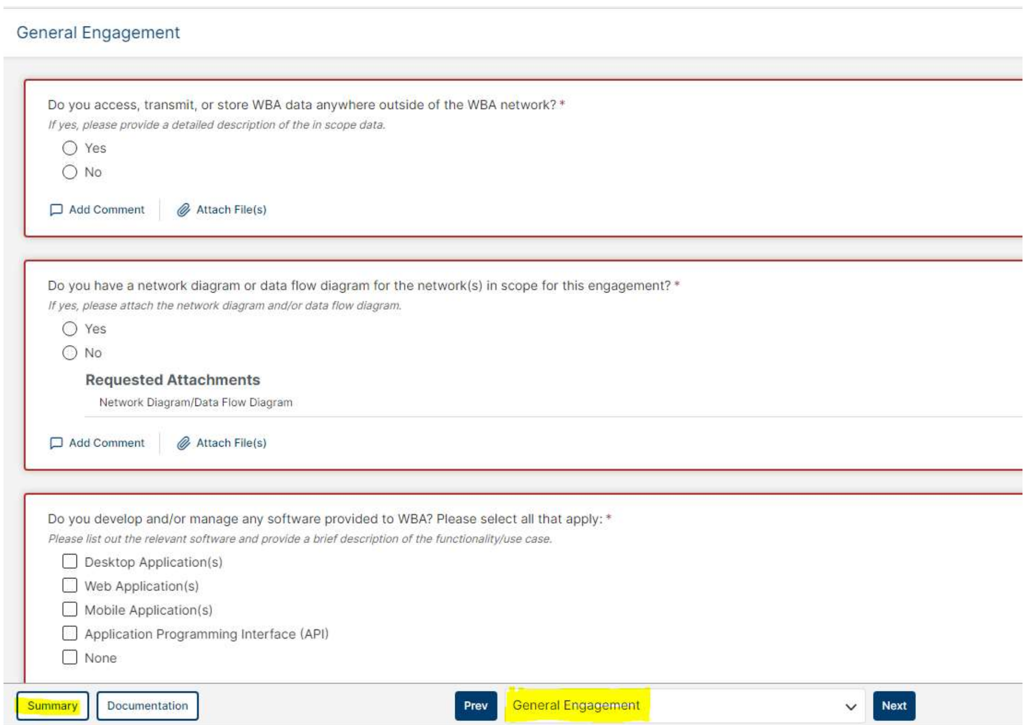


Questionnaire Summary

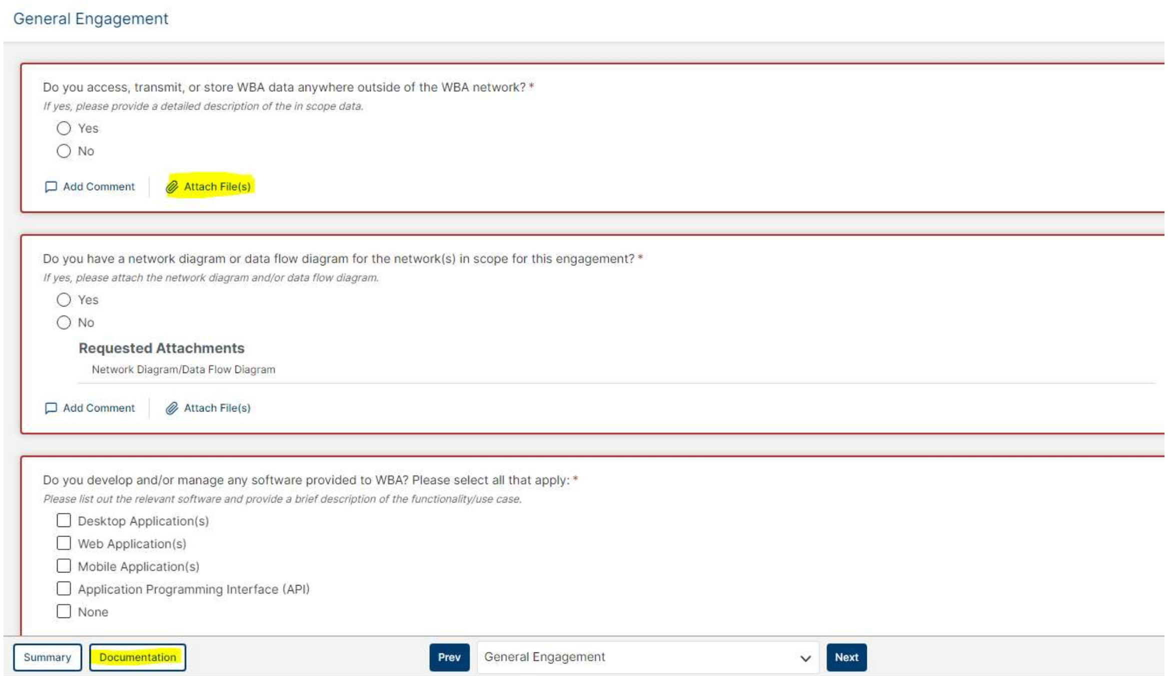
Section	Questions Answered / Total	Percent Complete
General Engagement	0 / 8	0 %
Asset Management	0 / 2	0 %
Secure Configuration	0 / 9	0 %
Vulnerability Assessment	0 / 4	0 %
Malware Protection	0 / 4	0 %
Network Security	0 / 2	0 %
Data Recovery	0 / 1	0 %
Skills & Training	0 / 5	0 %
Identity & Access Management	0 / 5	0 %
Boundary Defense	0 / 6	0 %
Audit Logging	0 / 3	0 %
Data Protection	0 / 7	0 %
Incident Response	0 / 6	0 %
Penetration Testing	0 / 3	0 %
Information Security Program	0 / 5	0 %
Facilities & Physical Security	0 / 2	0 %
Vendor Disposition	0 / 1	0 %

Summary Documentation Prev Summary Next

There are 17 potential control domains which may require your input. To navigate across each area, select the name of the control domain located below the SECTIONS heading. You may also use the drop-down at the bottom of the "Summary" section at the bottom center of the page.



Attaching files can be done either at the individual question level or via the “Documentation” button at the bottom left corner of the page.



Progress of the questionnaires can be viewed from the summary page by clicking the *Summary* button at the bottom of the main page. Once all questions have been answered and you are satisfied with your responses, please select the “Submit” button at the top of the questionnaire.

Test Assessment

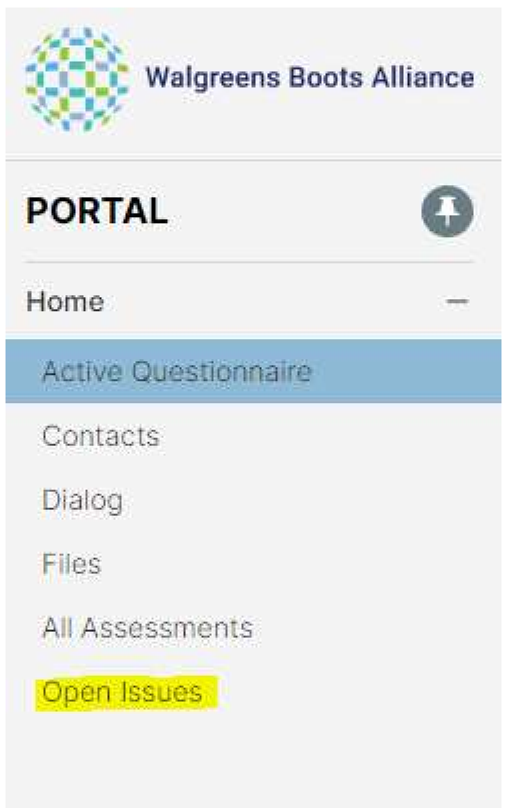
Print Import Export Submit

Questionnaire Summary

Section	Questions Answered / Total	Percent Complete
General Engagement	0 / 8	0 %
Asset Management	0 / 2	0 %
Secure Configuration	0 / 9	0 %
Vulnerability Assessment	0 / 4	0 %
Malware Protection	0 / 4	0 %
Network Security	0 / 2	0 %
Data Recovery	0 / 1	0 %
Skills & Training	0 / 5	0 %
Identity & Access Management	0 / 5	0 %
Boundary Defense	0 / 6	0 %
Audit Logging	0 / 3	0 %
Data Protection	0 / 7	0 %
Incident Response	0 / 6	0 %
Penetration Testing	0 / 3	0 %
Information Security Program	0 / 5	0 %
Facilities & Physical Security	0 / 2	0 %
Vendor Disposition	0 / 1	0 %

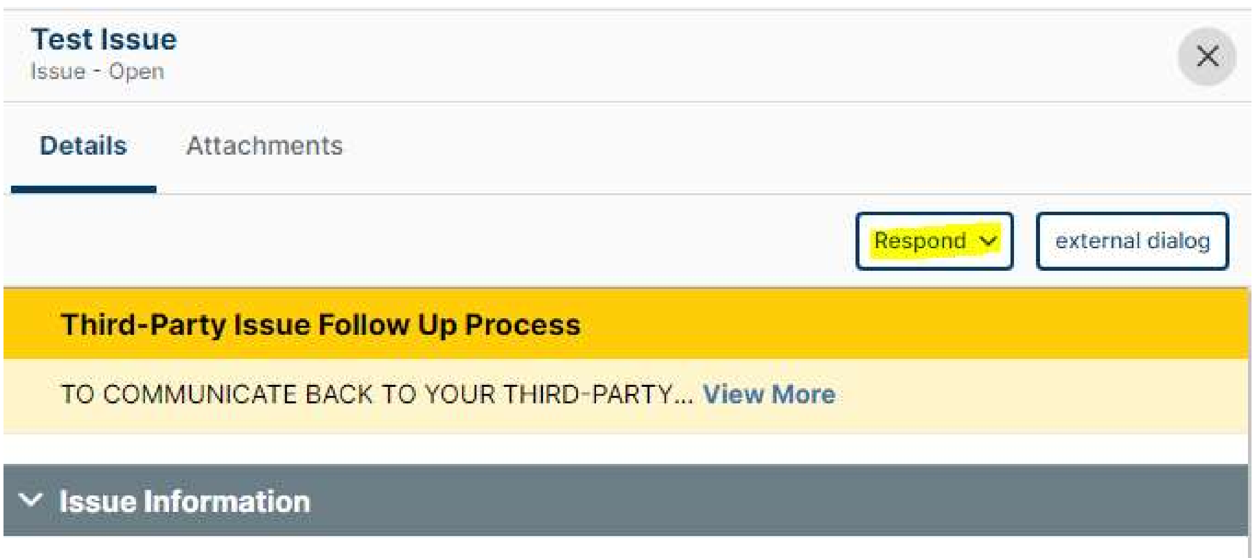
Findings Management

Upon completion of the assessment, findings may or may not be created. If findings are created, you will receive an automated email from system indicating that findings have been created with a link to access the findings in the system. The issues can be viewed and responded to in the “Open Issues” dashboard:



Once you click into the “Open Issues” dashboard, you will see a list of all findings associated with the assessment. We request that you provide a Remediation Plan for each finding identified or identify in writing that you will not be remediating the issue at hand.

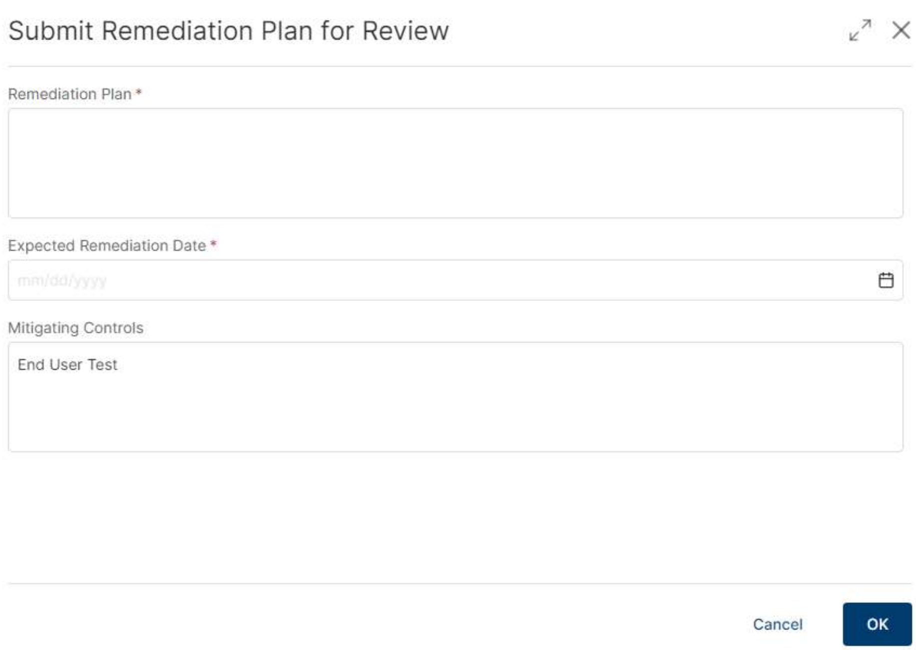
Remediation Plans or declines can be provided via the “Respond” button on each record:



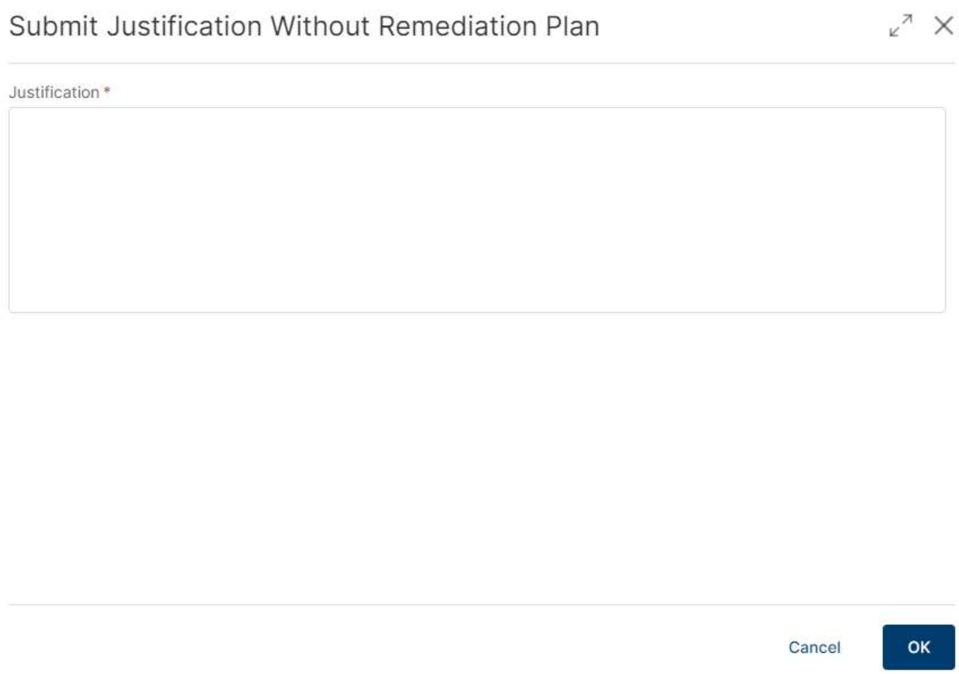
After clicking “Respond” you will have two options:

- Submit Remediation Plan for Review: For use if you plan to remediate the identified finding.
- Submit Justification Without Remediation Plan: For use if you either do not believe the finding is accurate or you do not plan to remediate the finding.

Submit Remediation Plan for Review:



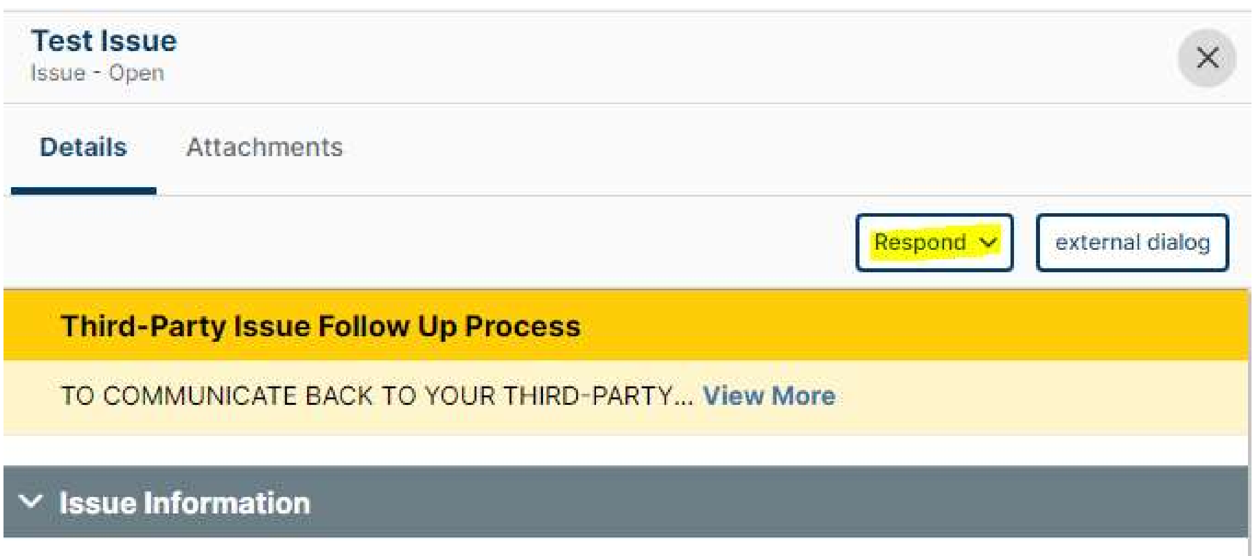
Submit Justification Without Remediation Plan:



Once the Remediation Plan is submitted, the Walgreens team will review the response and either accept the Remediation Plan or return the Remediation Plan requesting more detail. Once the Remediation Plan is Approved, it will move to a “Pending Remediation” status in the “Open Issues” dashboard. We expect that documentation is uploaded to the Finding record by the remediation date provided in the Remediation Plan. If you submit a Justification without Remediation Plan response, the information will be triaged appropriately, however, there is no further immediate action required on your part.

Submitting documentation for remediated findings can be initiated by attaching documentation to the “Attachments” Tab highlighted below:

Once the remediation documentation is uploaded, you can submit remediation evidence for review via the “Respond” button:



Once the remediation evidence has been accepted, you will receive an email notifying you that the issue is now closed, and it will be removed from the “Open Issues” dashboard.