Netskope guidance to Vendors using Thirdpartytrust

ThirdParty Trust is now a part of Bitsight

Introduction

This document is intended as a general overview and guidance on operating a vendors profile on the Thirdpartytrust portal. Netskope uses this portal for all its vendors who are determined to require initial and annual assessment of their security and privacy controls.

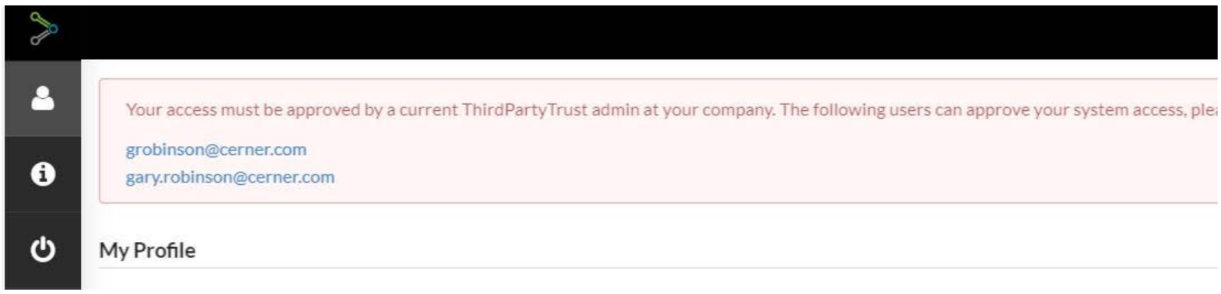
More information on ThirdPartyTrust is available on this link below
https://thirdpartytrust.atlassian.net/wiki/spaces/HEL/pages/508297283/Vendor+Training

Checking if your company already has linked to Thirdpartytrust

In some cases another person at your company (domain) may have already registered with ThirdPartyTrust and are in fact the administrators. In this case you will receive a similar message as below and you will need to reach out to these contacts in your company to approve your request. If these contacts no longer work for your company then we request that you reach out to vrm-support@bitsight.com for assistance.

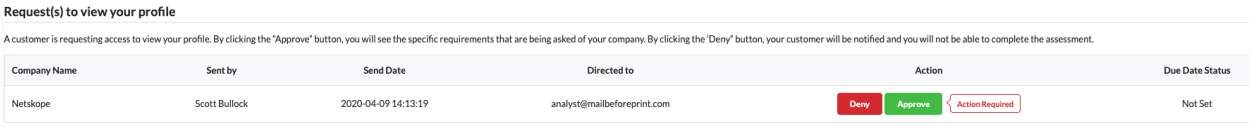
Hello,

I have created an account and am now presented with the following screen? Do I need to be given access before I can take appropriate next steps? I hav



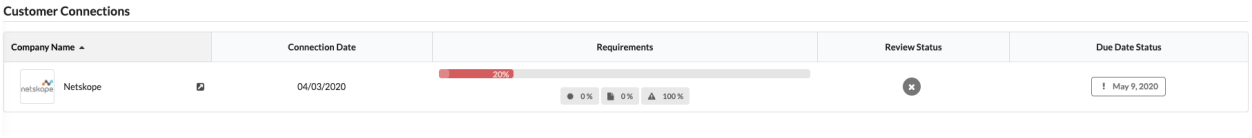
Accepting the connection from Netskope

Once you have registered on the Thirdpartytrust portal the next step is to ensure that you accept the connection request this will be found under the “Connections” tab



Once you approve you will see a progress bar at the top, this indicates your overall completion status as well as below showing the status of completion with Netskope.

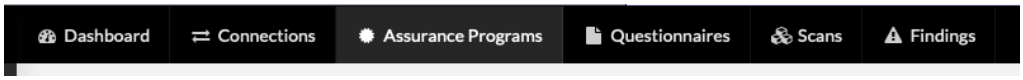
In this case Netskope has evaluated the need to ask for a number of assurance documentation



Managing Assurance Programs

Assurance programs contain a list of security evidence documentation that is required by Netskope as part of its vendor security/privacy due diligence program.

Firstly click on your “Assurance Programs” at the top of the screen to find out what elements are being asked for by each customer including Netskope.



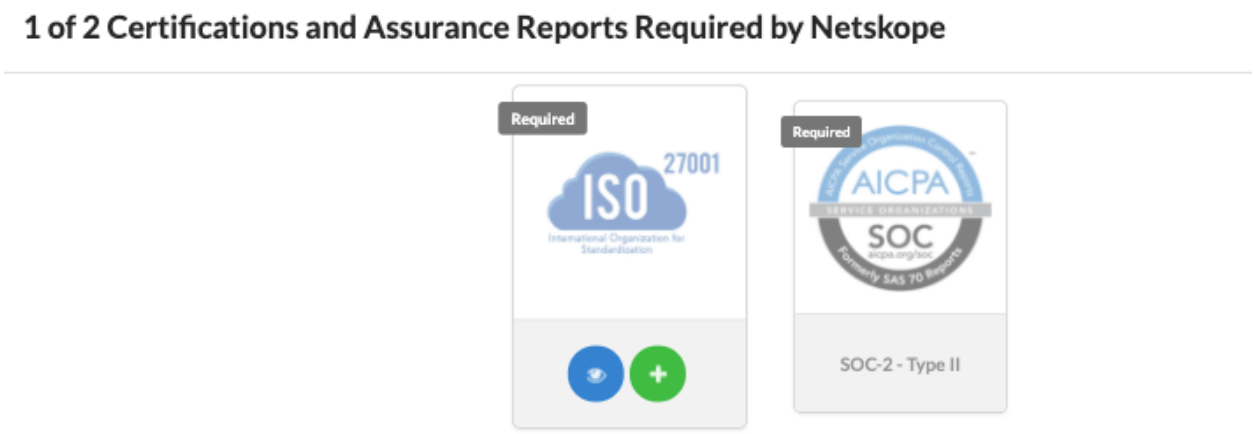
Certificates/Reports

To fulfil the requirements in this section Netskope are asking for a SOC 2 type 2 report or an ISO 27001 Certificate.
Please note : Netskope will not accept any certificates or reports from your service providers , for example you cannot claim ISO 27001 certification or SOC 2 Type 2 based on AWS’s reports , these MUST be your companies certificates or reports for your delivered services to Netskope.
In this example let's say your company only has a SOC 2 Report .

Click on the box and an “eye” icon will appear

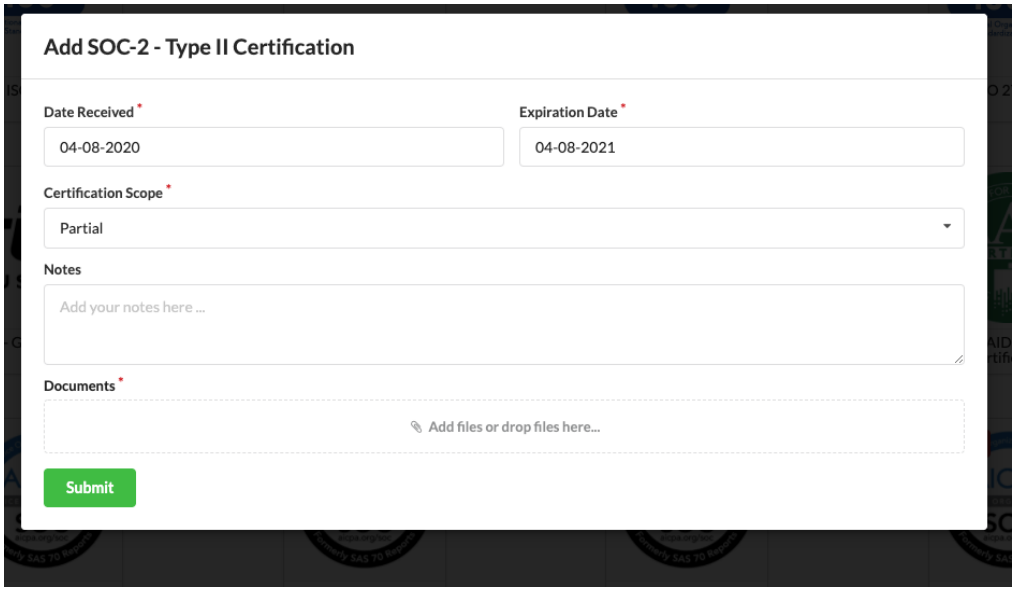
Now click on the “eye” icon to open up and show the requirements that have been asked for by Netskope.

Hover your mouse over each item and it will allow you to



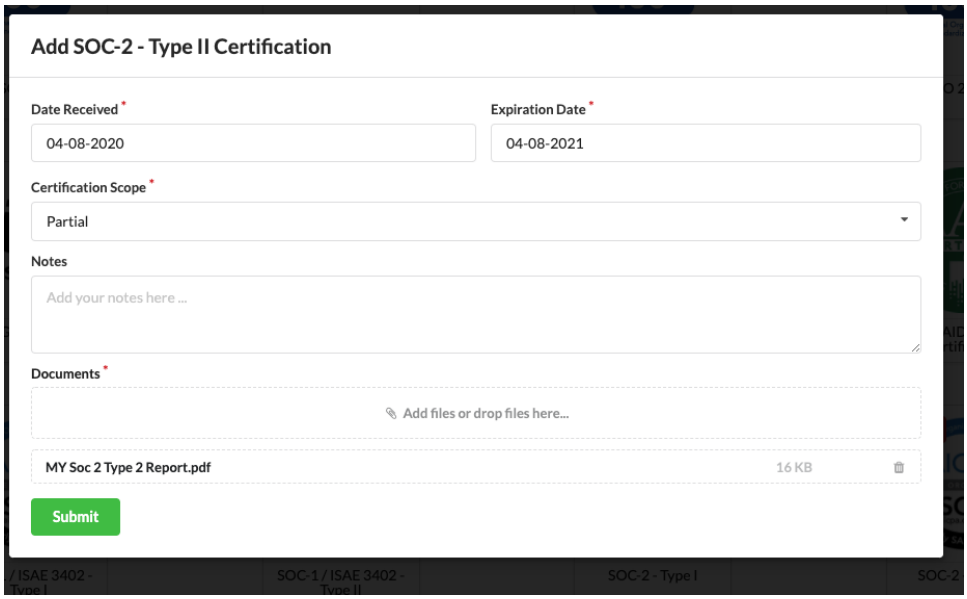
SOC 2 Type 2 Report Submission

Click the + icon under the SOC 2 Type 2 - this will open up the section where you will need to complete the entry of your SOC 2 Type 2 report.

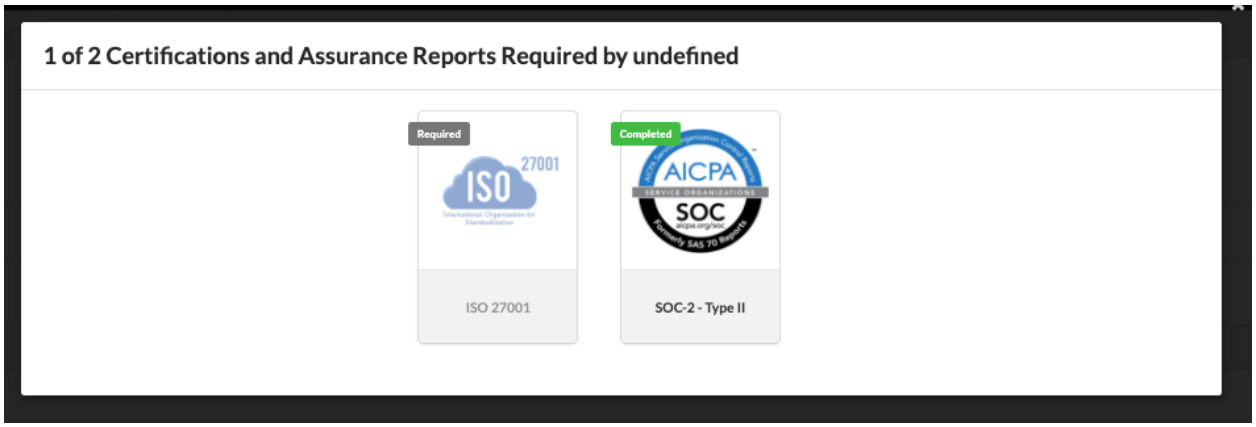


Review your SOC 2 Type 2 report and it should have an issue date - enter that in the “Date Received” section and as SOC 2 Type 2 reports are normally updated annually enter the expiration date as 1 year from the date received . This is important to get this right otherwise the report may be rejected by the customer.
Select the scope of the certification/report , either partial or full . However be aware that the report must be scoped to the delivery of the services you are providing to Netskope.

If your SOC 2 Type 2 report is older than 6 months Netskope requires you to provide a bridge letter to attest that the controls are still effective. Failure to provide
Drop your SOC 2 Type 2 report into drag/drop area where it asks for the report -enter any relevant notes you believe are pertinent to the report.



The example above shows a completed SOC 2 Type 2 - Click submit and you have now completed part of the assessment.

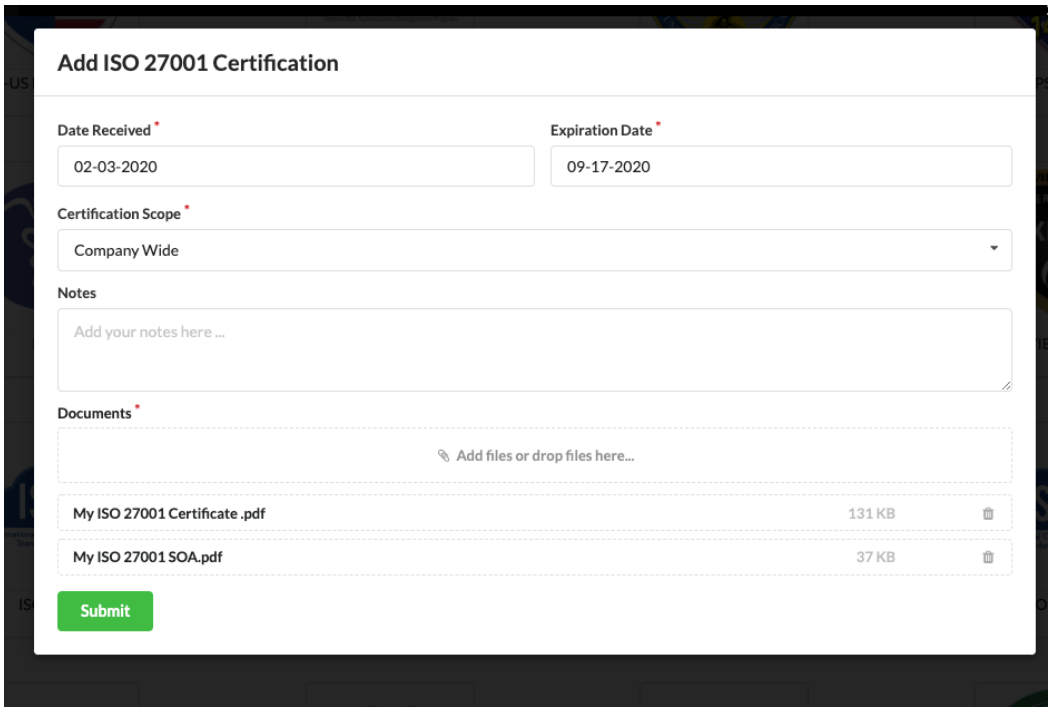


ISO 27001 Certificate Submission

If your company has an ISO 27001 Certificate for your services - click add and select ISO 27001

Date received is the date you first received your ISO 27001 certificate and the expiry date would be the same as what is shown on your certificate.
Do not deviate from the expiry date on the certificate, doing so we cause the customer to raise a finding on the certificate and reject it .
Select the scope of the certificate either partial or company wide - add any notes you feel are relevant to support the certificate.

Drop the certificate file into the drag/drop area
If you are adding an ISO 27001 certificate Netskope mandates that you also to add the Statement of Applicability in order for the Netskope to ensure that the scope of the controls that were assessed for the certificate are complete.



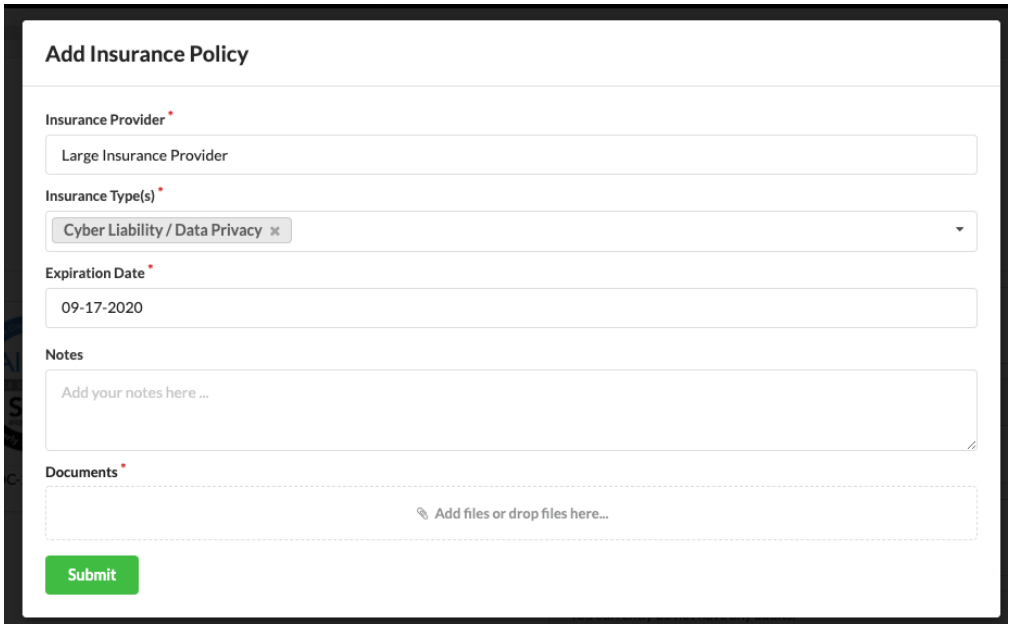
Click submit and the certificate section is complete

DO NOT add blank files or attempt to claim any certificate or report without the evidence as shown above. These will be immediately rejected by Netskope .

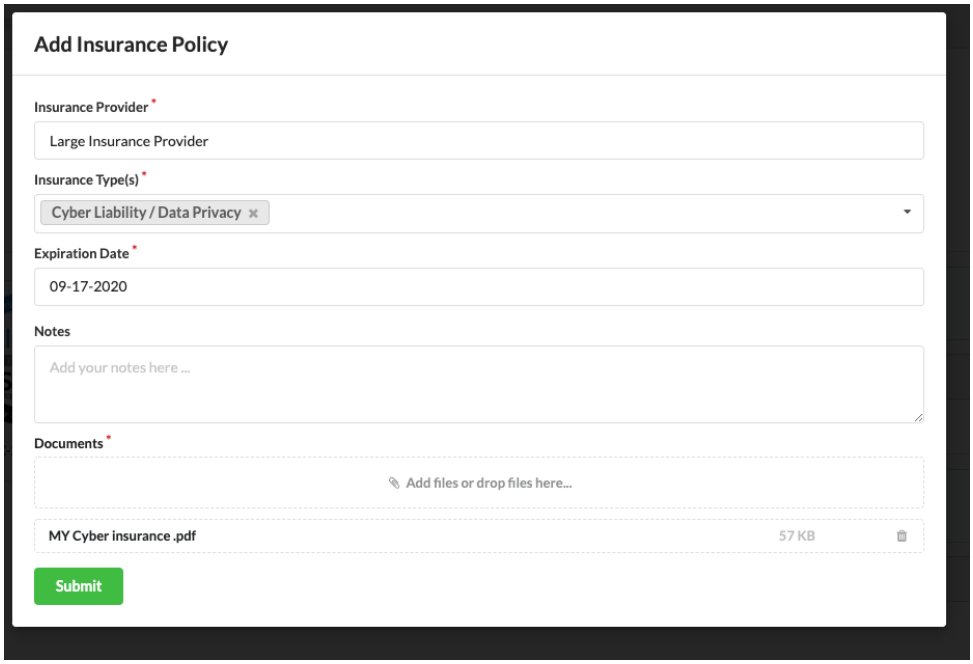
Evidence of Insurance Submission

Netskope are now asking for evidence of your cyber liability/data privacy insurance.

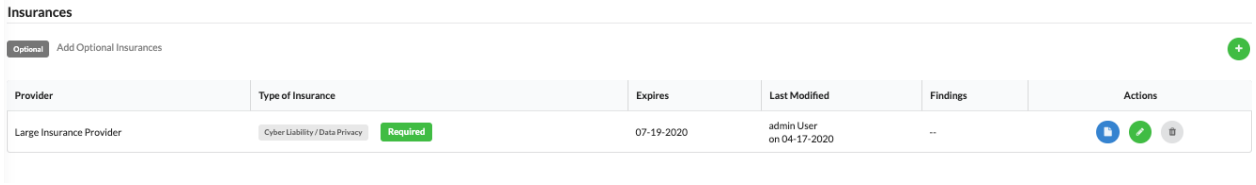
Click the + green icon on the right hand side of the page to add insurance.
Enter the Insurance provider and select the Insurance type - make sure this is cyber liability/data privacy and enter the expiry date - this would normally be 1 year after the issuance of the policy - but make sure this is entered correctly



Now drag/drop the insurance document and click submit

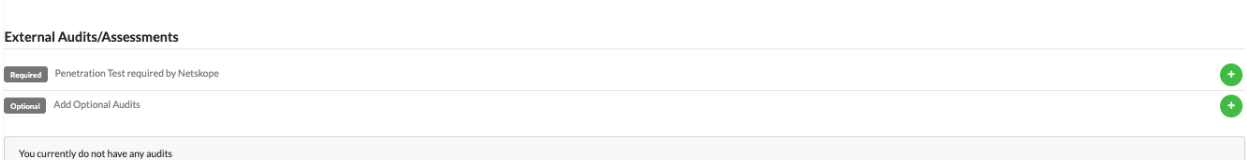


Don't worry it it still tells you it needs insurance - this normally updates within 30 seconds - as you can see below its telling you the insurance is completed

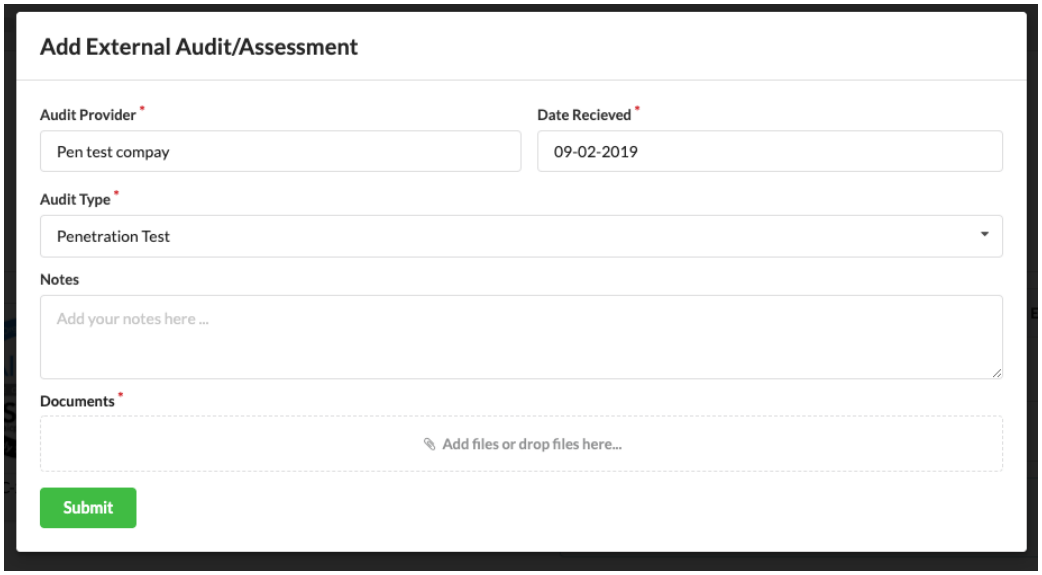


Penetration Test Evidence Submission

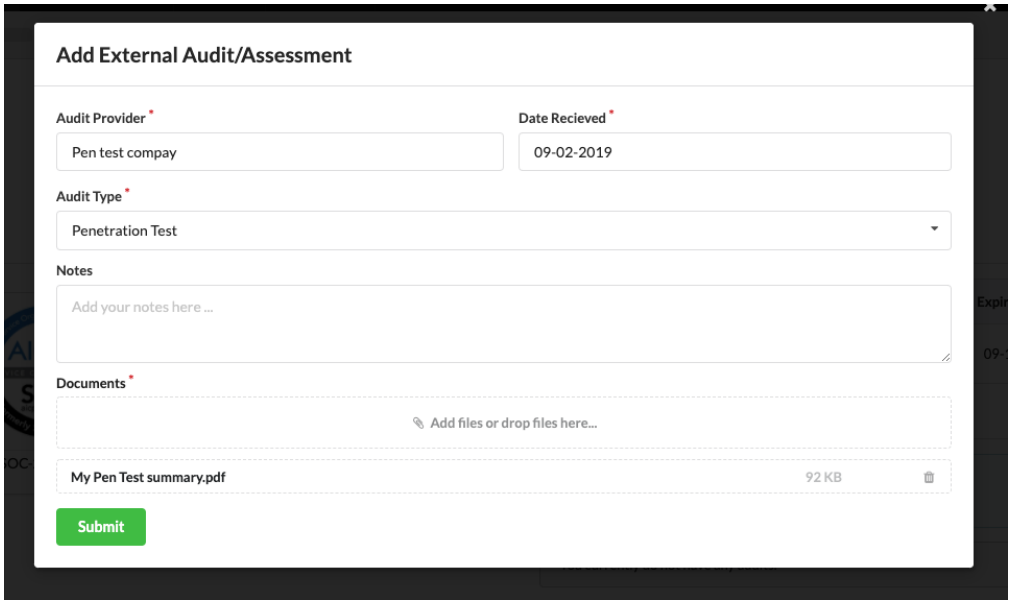
Netskope will accept either a full penetration test report or an executive summary report however if there are any findings in the summary higher than “Low Risk” we expect either a remediation report or attestation from you to explain if the findings are remediated or a timeline for remediation.



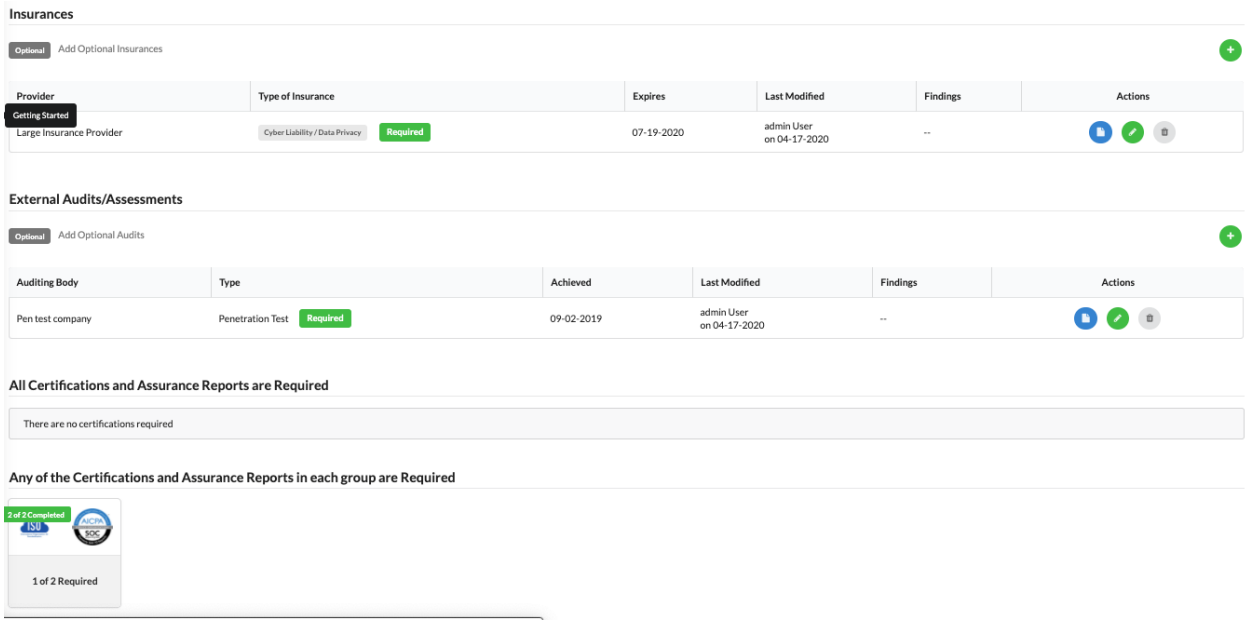
Click the green + icon on the right hand side of the page to open up the entry box shown below
Enter the name of the penetration test provider, when the report was received and choose the audit type “Penetration Test”



Drop in the penetration test document , and as above if there is a remediation summary or attestation letter then drop that in as well .
** Note : Penetration tests older than 1 year will be rejected


Add External Audit/Assessment
Audit Provider *
Pen test compay
Date Recieved *
09-02-2019
Audit Type *
Penetration Test
Notes
Add your notes here ...
Documents *
Add files or drop files here...
My Pen Test summary.pdf
92 KB
Submit

Now you can see that all the requirements in the assurance section have been completed

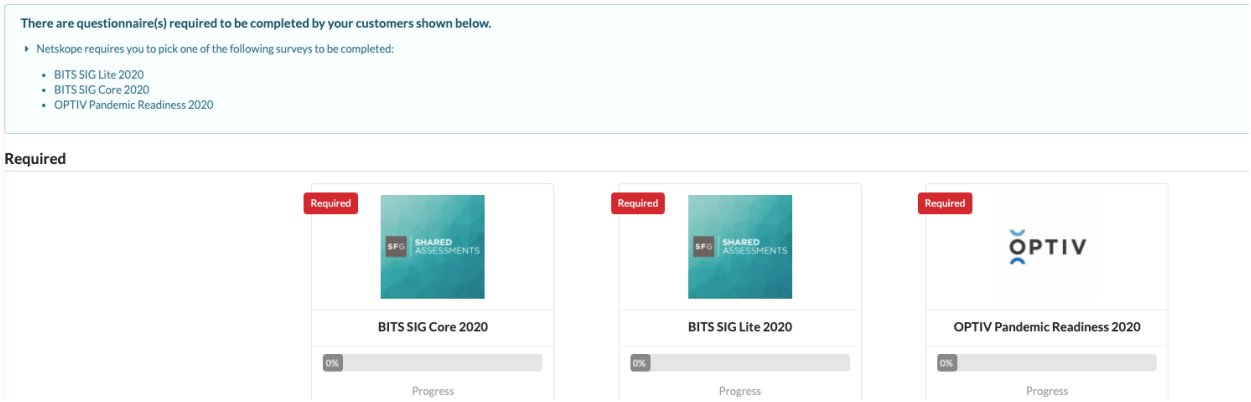


Watermarking documentation

Remember submission on the Thirdpartytrust portal is not only for the usage of Netskope but can also be used to share your evidence to other customers in an easy to consume manner and potentially reduce your customer/vendor burden. Therefore as the documentation is likely to be used by other customers we strongly recommend that documentation is not watermarked for example (for Netskope usage only)

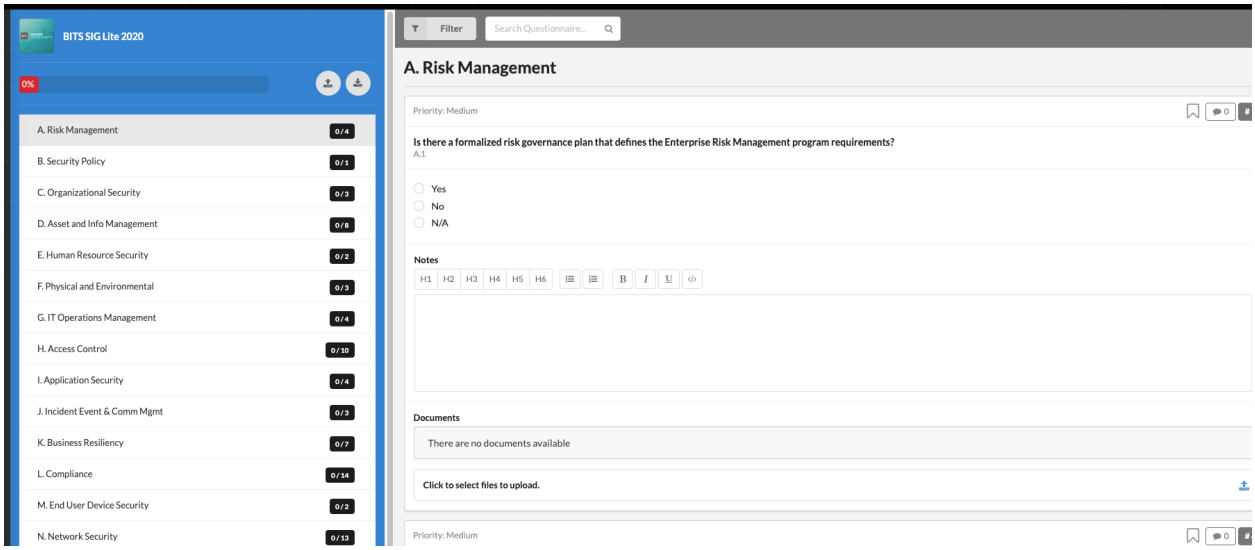
Questionnaires

Netskope requires a number of questionnaires to be completed - in this example case as a medium risk SAAS provider we are actually asking for either a SIG lite 2020 or SIG Core 2020 to be completed. The pandemic questionnaire is mandatory



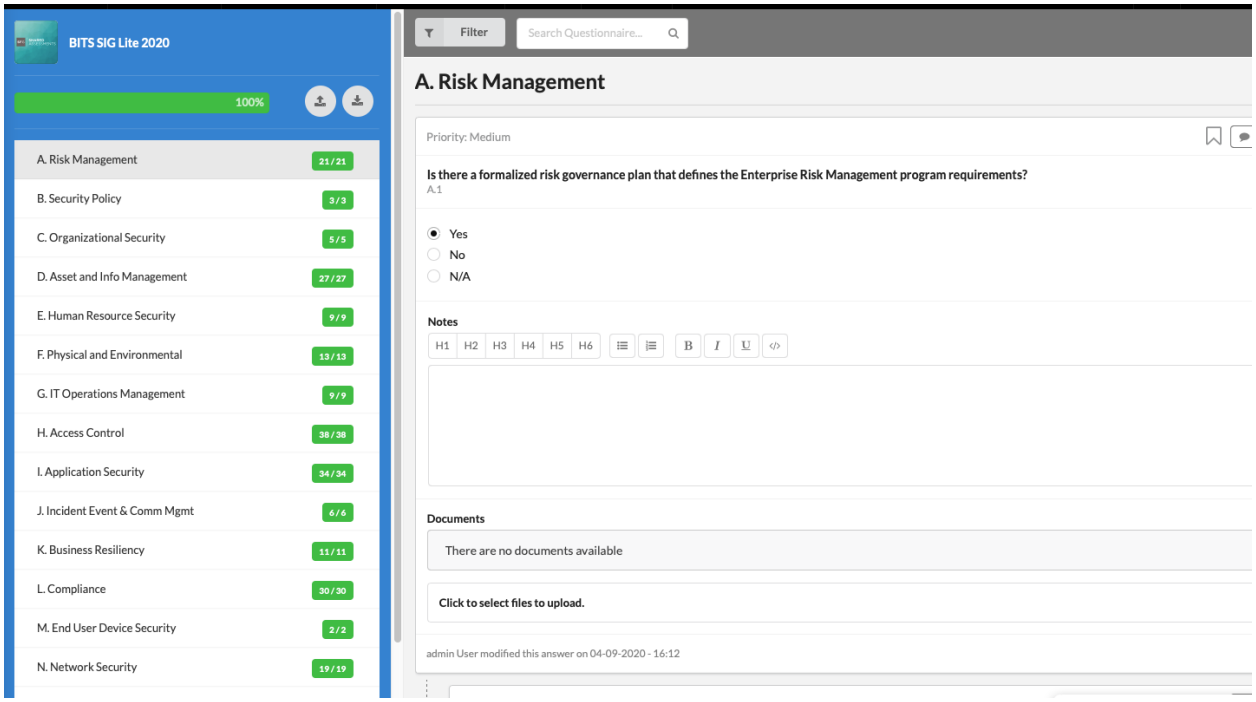
Vendors can choose either a SIG Full or Sig Lite . In this example just the SIG Lite 2020 will need to be fulfilled - click on the SIG Lite 2020 and it will open up the full questionnaire- . For the first/initial audit/assessment Netskope will only require a simple yes, no or not-applicable answers.

If you already have a completed SIG that is recent this can be sent to vrm-support@bitsight.com who will assist in uploading the document.
Do not attempt to upload your own SIG as the formats may not be the same and you will receive an error message. The upload/download feature is there for you to work offline with the SIG, firstly download the SIG and once complete upload the pre-formatted document.
You should expect the SIG lite to take around 1-2 hours to complete - but remember once this is done for one customer you don't need to do it again for the next one !



Answer each question carefully , be prepared to be asked for backup evidence to support your answers as Netskope may choose to sample-audit in detail some vendors.

Once every question has been answered the progress bar should show 100% as shown below.



Complete each questionnaire in order- once you have completed all of them you should see the progress bar for all requirements.

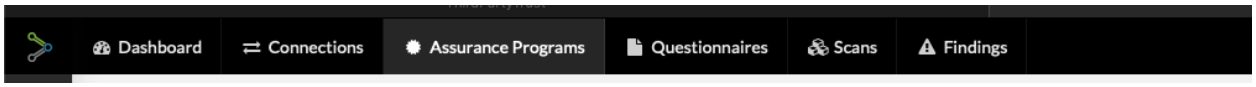
Once you have completed all the requirements , or have submitted all the information that you have available - send a message to grc@netskope.com informing Netskope you have completed the submission and it is ready for review

Review Process

Once you have submitted your documentation and completed the questionnaires Netskope will review the evidence and where appropriate raise findings against the documentation.

Handling Findings

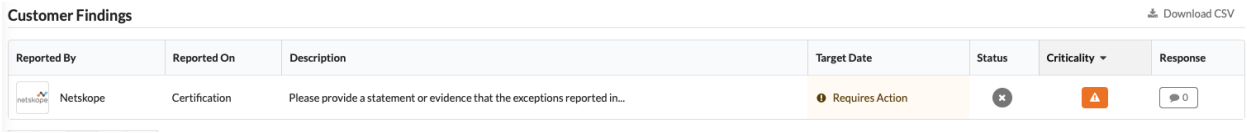
Findings will alerted via email to the registered user via email and also show up on the findings tab of the vendor's Thirdpartytrust portal



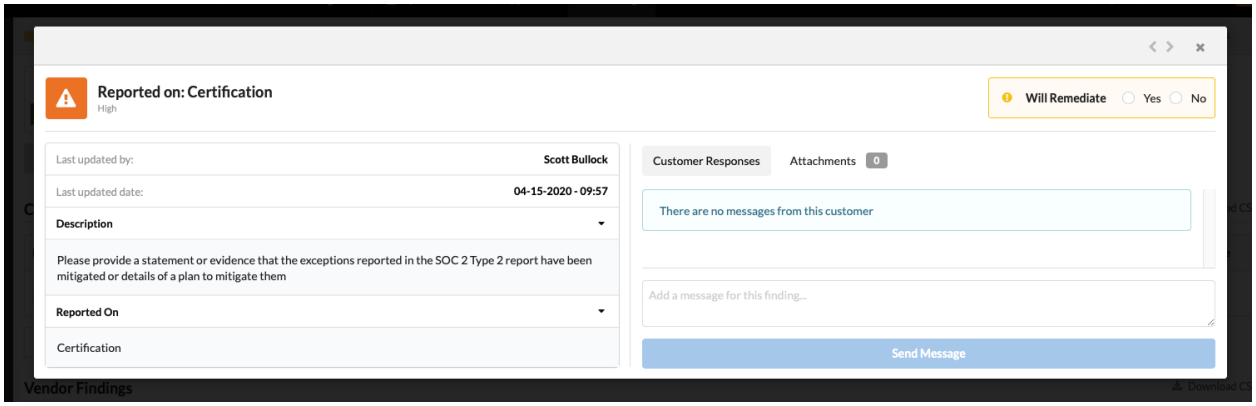
There are a number of issues that Netskope may escalate a finding , below are a few examples of how to manage/handle these findings.

Example 1 : SOC Report Exceptions

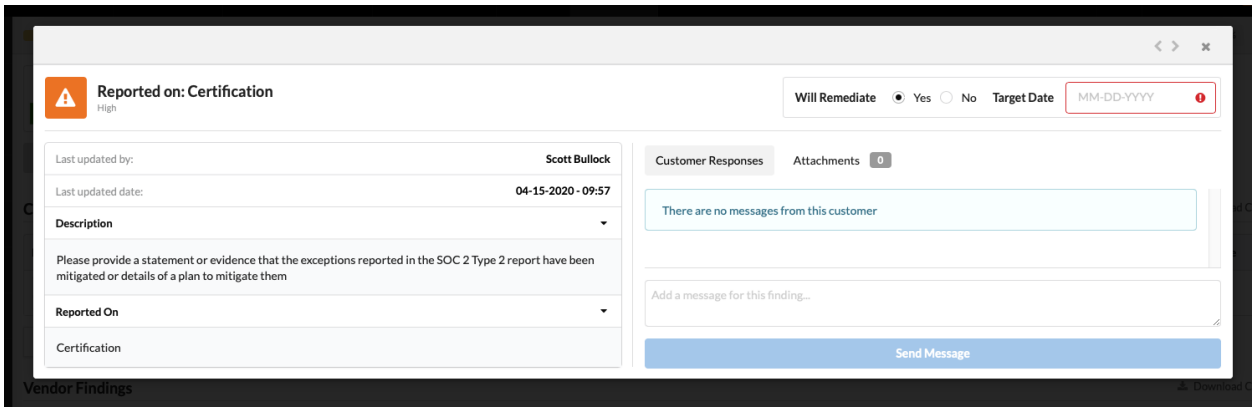
Netskope will review the SOC reports submitted and may choose to request clarification of any reported exceptions to ensure that mitigations are put in place.
Netskope have raised an exception against the SOC report as show below



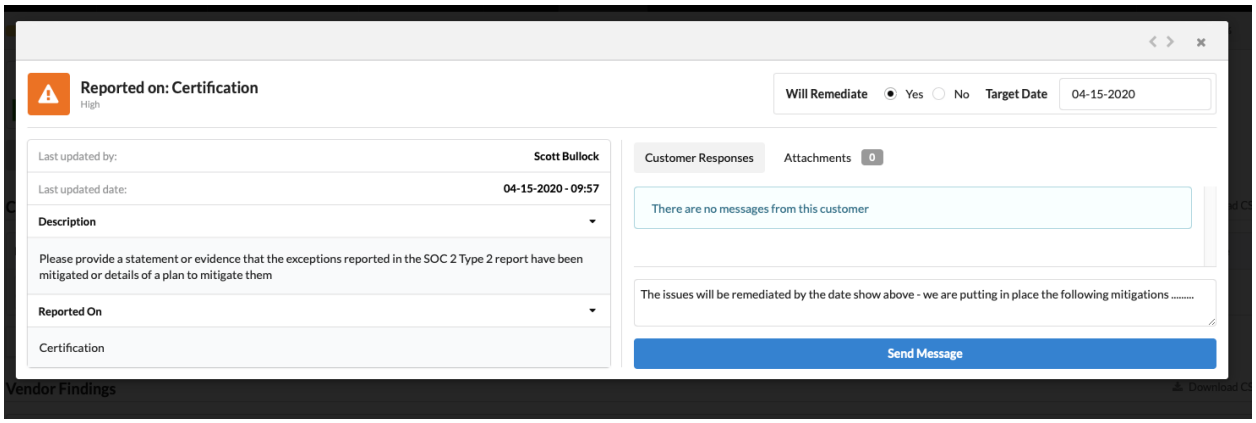
Click on the description and this will open up the full message



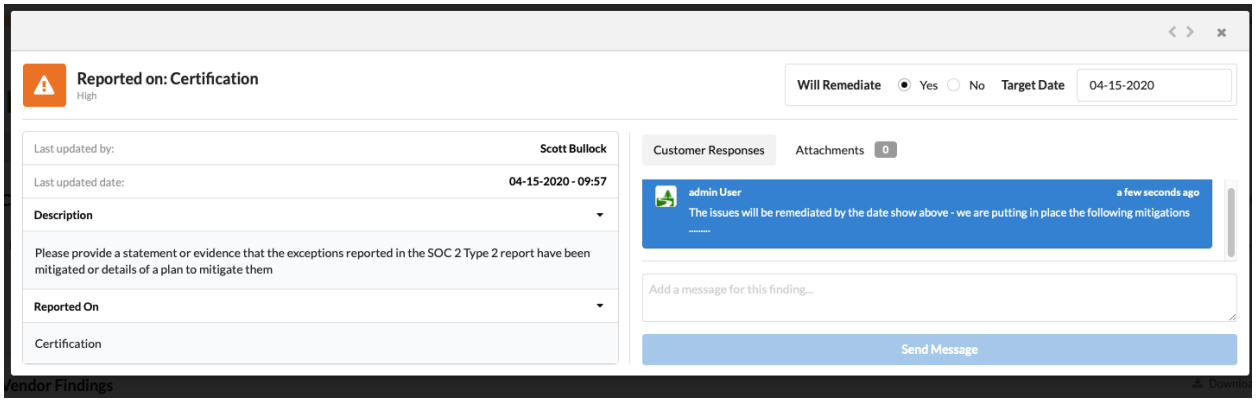
Netskope is asking for evidence or a statement on the exceptions found in your soc report , firstly you must indicate if you are intending to mitigate or not . If the exception has already been addressed select “Will Remediate” - this will open up a target date



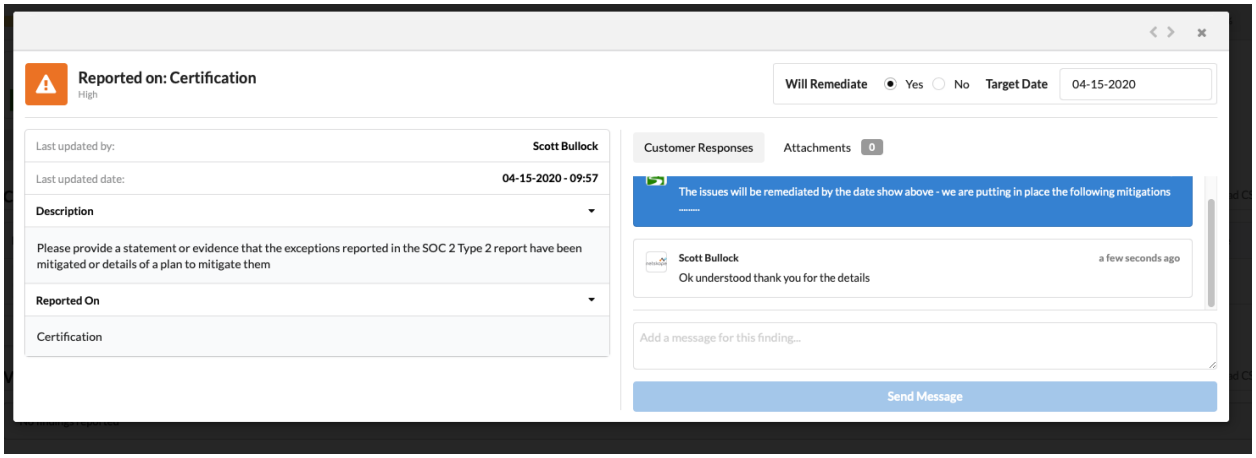
Enter a date and add a message explaining the mitigation strategy



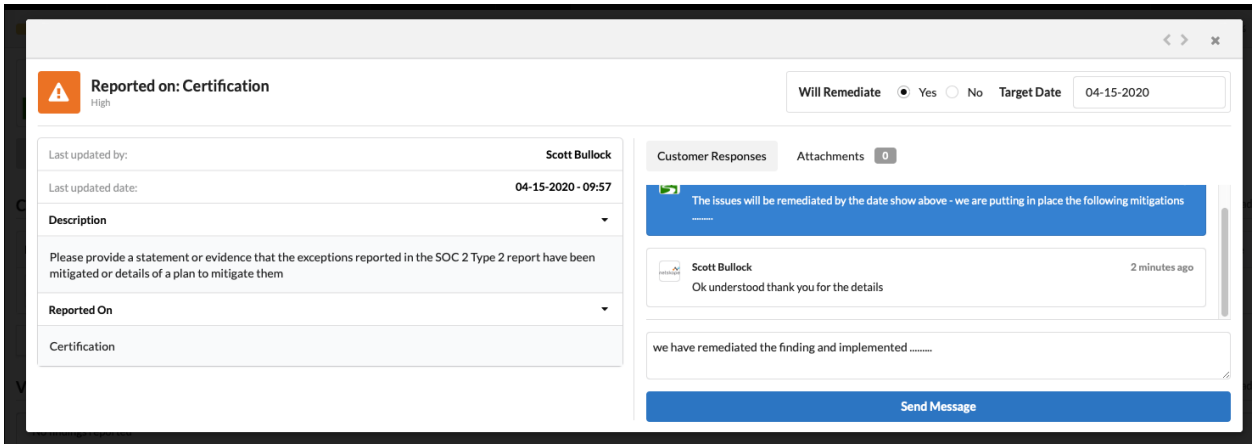
And finally press send message - the message will show sent and will be received by Netskope to review



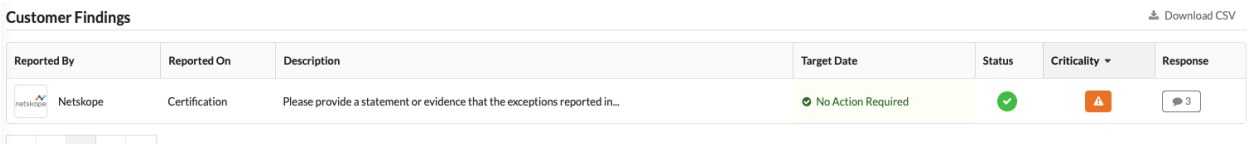
In this case Netskope responds thanking the vendor for the update



Once the issue is resolved send a further message indicating the remediation has been completed should be submitted



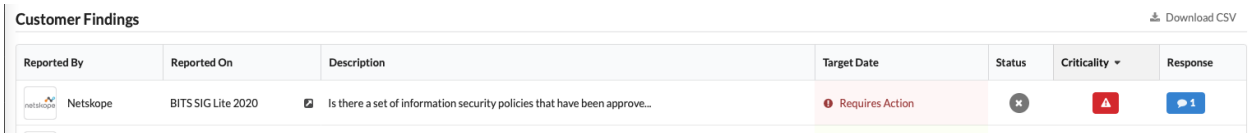
This will then be sent to Netskope who will review the statement and once this has been accepted the target date will be updated to “No Action Required” and status will show completed as shown below



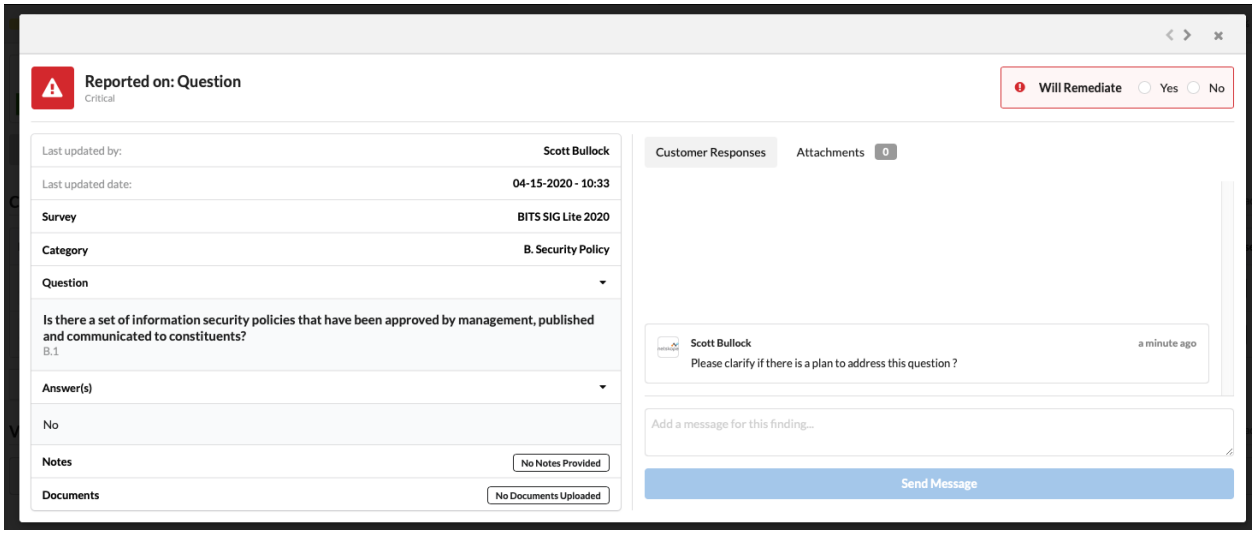
This finding has now been successfully resolved and accepted by Netskope

Example 2 : SIG Questionnaire issues

Netskope will review the answers supplied in the questionnaires and may choose to request clarification/correction or additional information on a question. In this case Netskope has flagged up a question in the SIG

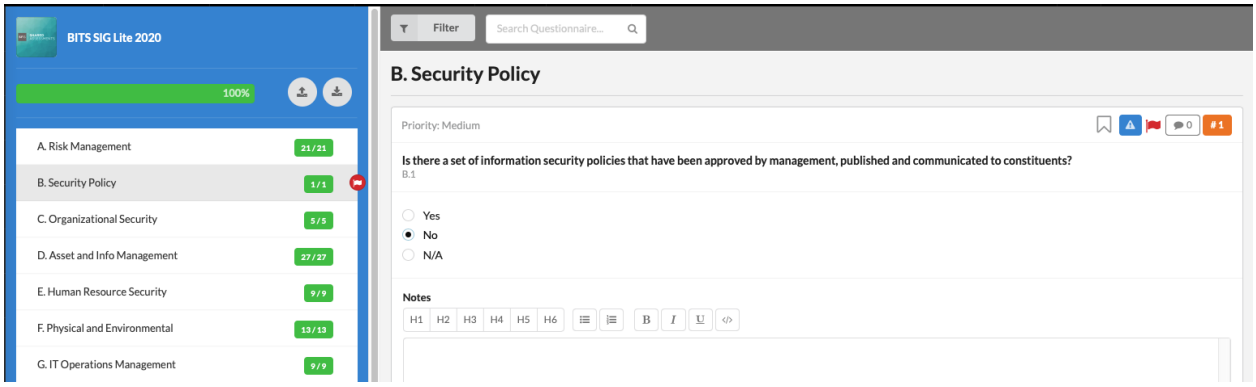


Clicking on the item shows the detail as to precisely which question need addressing

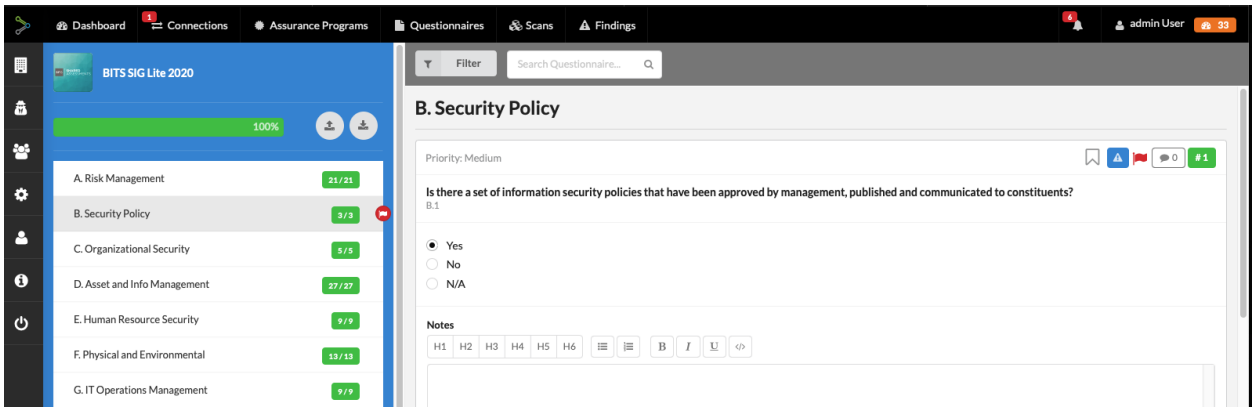


Again enter the remediation date and send a message detailing what will be the mitigation action. In this case this question was answered incorrectly.

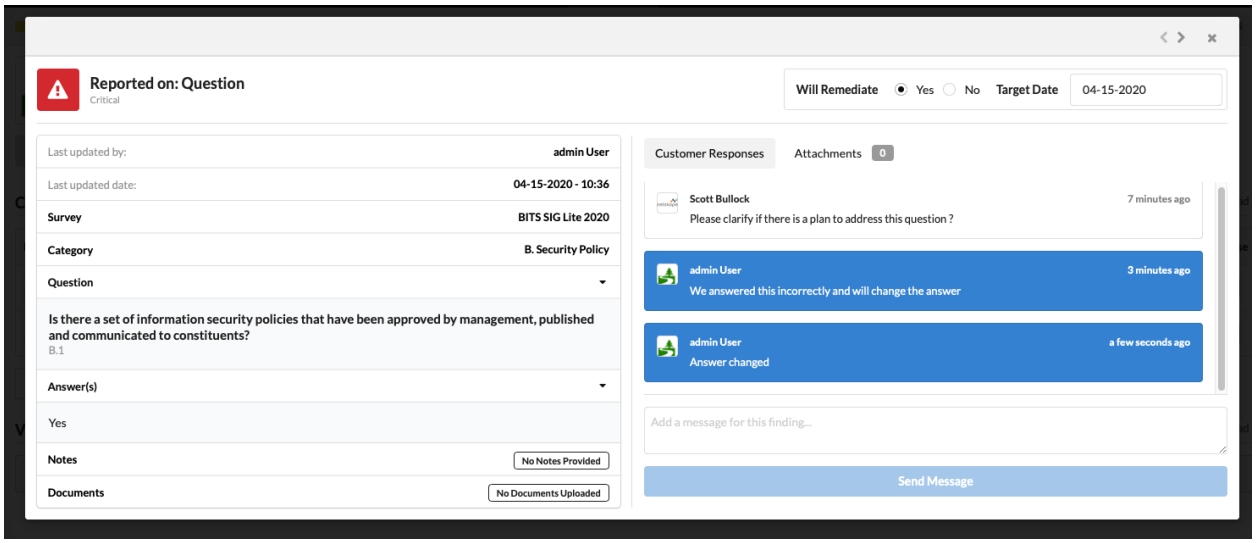
Opening up the SIG Lite 2020 questionnaire now shows where the issue was flagged



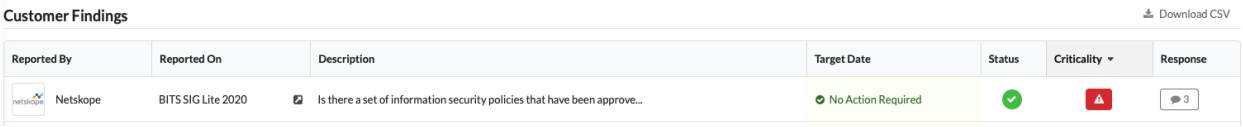
We now correct the answer



Return to the findings and submit a message to let Netskope know the answer has been updated

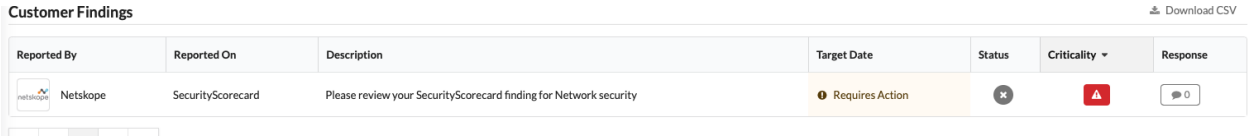


Once Netskope has reviewed the finding and accepted the response the finding will show as completed with no action required

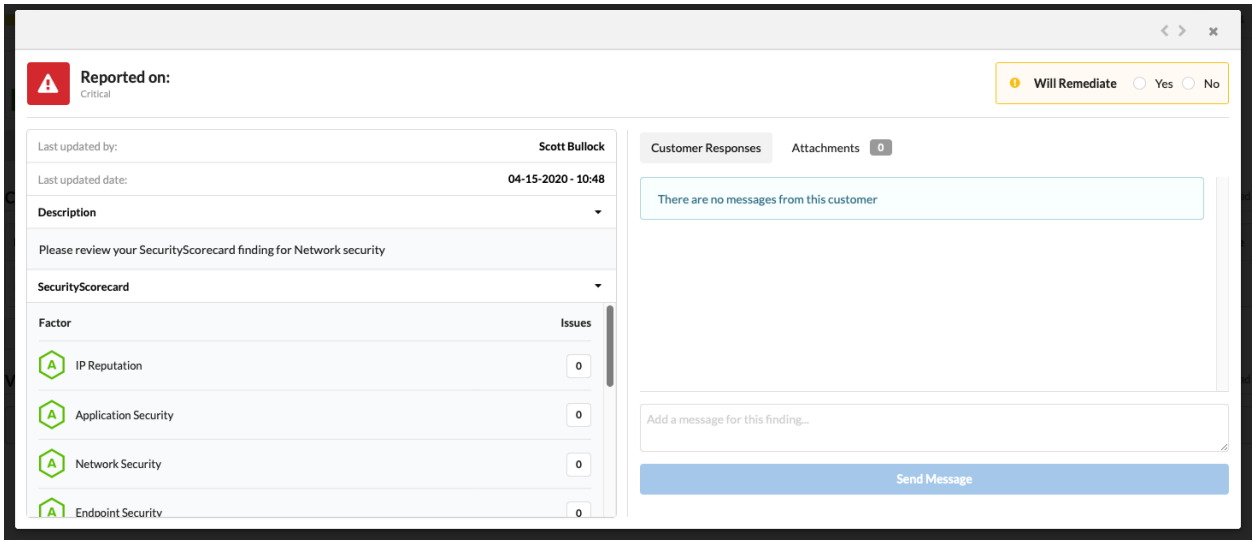

Customer Findings
Download CSV
Reported By
Reported On
Description
Target Date
Status
Criticality
Response
Netskope
BITS SIG Lite 2020
Is there a set of information security policies that have been approve...
No Action Required
3

Example 2 : Poor SecurityScoreCard

Netskope will review the SecurityScoreCard reports as part of the review and may create findings based on the scoring.



Opening up the finding will show in detail



There are a number of strategies to improve the SecurityScoreCard Report. Detailed reports can be obtained by purchasing the full report from the “Scans” Section
Vendors are recommended to keep track of their SecurityScoreCard profile as Netskope uses these scores as part of the component to compile the total risk score of a vendor.