BISHOP FOX®

8240 S. Kyrene Road
Suite A-113
Tempe, AZ 85284

P 480 621 8967
F 480 383 6401
www.bishopfox.com

LETTER OF ASSESSMENT FAQ

What is a Letter of Assessment?

A Letter of Assessment is a document that you can share with your customers to prove that a proper security assessment has been conducted. The most common reasons to obtain a letter of assessment include:

- Satisfying customer security requests
- Meeting compliance requirements
- Demonstrating due diligence

Bishop Fox provides these letters in PDF format, which are digitally signed by an authorized Bishop Fox partner and cannot be modified.

Letters of Assessment are not intended to be marketing documents or replace the details of a report. Although reports may include opinions on the security of tested targets, Letters of Assessment do not attest to or provide opinion regarding the overall security of tested targets. Letters only serve as evidence that proper testing has been performed.

As you may suspect, we are very strict in terms of when we are comfortable issuing Letters of Assessment. One poorly delivered Letter of Assessment can jeopardize the trust inherent in all of the Letters of Assessment that we have ever issued and may jeopardize any Letters of Assessment we issue in the future. Our strictness ensures that both our clients and their customers have a high level of confidence when reviewing a Bishop Fox letter.

Can we share the Letter of Assessment with our customers?

Yes, we encourage it. If they would like for the letter to be sent directly from us, we can do that for you as well.

Will you speak with our customers about the letter and type of testing performed?

Yes, we are happy to discuss our testing approach and methodology.

Are there different types of letters?

Yes. While the letters are purposefully simple, four letter variations can be provided.

Letter Variations		
Type 1	• States an **assessment** was performed	See appendix for a sample letter
Type 2	• States an **assessment** was performed • Includes **number of identified vulnerabilities** (i.e., critical-, high-, medium-, and low-risk)	See appendix for a sample letter
Type 3	• States an **assessment and remediation testing** were performed	See appendix for a sample letter
Type 4	• States an **assessment and remediation testing** were performed • Includes **number of identified and remediated vulnerabilities** (i.e., critical-, high-, medium-, and low-risk)	See appendix for a sample letter

Is there a difference in cost for the different versions?

No. We do not charge to create different versions after an engagement has been completed.

Be aware that we cannot provide a letter describing the state of security after remediation unless our team performs the remediation testing. If remediation testing was not included in the original scope of work, then additional effort must often be added to the scope before a letter with remediation details can be shared.

Can we have more than one version?

Yes. It is fine to ask for different versions, and many of our clients do. It is not uncommon for our clients to selectively share different letter types based on their customers' requests.

Can I change or modify the Letter of Assessment?

You may request edits if you discover a typo or an inaccuracy, but otherwise the language and format of the letter cannot be altered.

What if we fix an issue while testing is still occurring?

If we find it, we will report it. However, if it has been remediated by the time the testing is complete, and we are able to retest to confirm proper remediation, then we will update the LOA to report the issue as having been found but also remediated.

What if we change the environment or change code during testing?

We strongly discourage changing the testing environment or the codebase during testing. We also request that our testing not be obstructed or hindered. During the course of the testing, the engagement team must be able to achieve a high level of confidence in the results.

If we determine that changes or obstructions are significant and substantive, then it will be **boldly** noted in the letter. If the disruption is too severe, we may decline to issue a letter.

The determination of what qualifies as a significant change is made at Bishop Fox's sole discretion, but as a general guideline, if it materially affects the results of the testing, then it is significant. In all circumstances, the contents of the letter must stand up to any questions from a third party who may be reading and evaluating the letter.

What if we stop the testing early?

A letter will not be provided. The engagement must run to completion. To avoid any confusion, the scope for your project is commensurate with the level of effort required to issue a Letter of Assessment. So, if you want a letter at the end of the project, we have to be comfortable that a proper test has been performed before issuing one.

What if we don't test against production?

That is OK. The environment being tested is noted in each Letter of Assessment.

Can you create a Letter of Assessment for us retroactively?

Under very limited circumstances, we can create a letter of assessment if the previous testing meets or exceeds the level of confidence needed. The dates on the letter will indicate when the testing was performed.

We do not issue letters if significant changes have been made to the target or more than six months have passed since the assessment was performed.

Is the Letter of Assessment included in the Project Fees?

Yes and no. Letters of Assessment are held to the same standards as our other deliverables, but in the spirit of not nickel-and-diming our clients, they are really not factored into the cost of the project.

To further clarify, if you wanted to take out the letter, the price would be the same. If we quoted this project without a letter and you would like to add one, the cost would be the same, assuming the scope allows us to achieve the necessary level of confidence in testing.

Why don't you make a statement about whether we are "secure"?

Our assessments are always scoped to be commensurate with the complexity of the environment, but the term "secure" is too subjective to withstand any level of educated questioning. Furthermore, any informed customer who reads a letter stating that a system is "secure" will actually have more doubts about the security of the system than if it was omitted.

APPENDIX A — LOA SAMPLES

The following pages are examples of the different types of LOAs Bishop Fox offers.

Letter of Assessment Type 1

8240 S. KYRENE ROAD
SUITE A-113
TEMPE, AZ 85284
UNITED STATES

WWW.BISHOPFOX.COM

February 31, 2050

Acme Corporation
10 Ton Parkway
Albuquerque, NM 12345
United States

To Whom It May Concern:

In February of 2050, pursuant to our agreement with Acme Corporation, the Bishop Fox assessment team conducted a hybrid application assessment of the Acme application.

The assessment objective was to identify, within the designated time and scope, any security issues in the Acme application. The assessment team combined automated application vulnerability scanning, code review, and manual penetration testing techniques in order to rapidly locate attack vectors and simulate real-world exploitation.

Acme has been provided the detailed findings and recommendations resulting from the assessment in an assessment report.

Sincerely,

Vincent Liu
Partner
Bishop Fox

Letter of Assessment Type 2

8240 S. KYRENE ROAD
SUITE A-113
TEMPE, AZ 85284
UNITED STATES

WWW.BISHOPFOX.COM

February 31, 2050

Acme Corporation
10 Ton Parkway
Albuquerque, NM 12345
United States

To Whom It May Concern:

In February of 2050, pursuant to our agreement with Acme Corporation, the Bishop Fox assessment team conducted a hybrid application assessment of the Acme application.

The assessment objective was to identify, within the designated time and scope, any security issues in the Acme application. The assessment team combined automated application vulnerability scanning, code review, and manual penetration testing techniques in order to rapidly locate attack vectors and simulate real world exploitation.

Acme has been provided the detailed findings and recommendations resulting from the assessment in an assessment report, which includes one high-risk vulnerability (one instance), two medium-risk vulnerabilities (two instances), and three low-risk vulnerabilities (three instances).

Sincerely,

Vincent Liu
Partner
Bishop Fox

Letter of Assessment Type 3

8240 S. KYRENE ROAD
SUITE A-113
TEMPE, AZ 85284
UNITED STATES

WWW.BISHOPFOX.COM

February 31, 2050

Acme Corporation
10 Ton Parkway
Albuquerque, NM 12345
United States

To Whom It May Concern:

In February of 2050, pursuant to our agreement with Acme Corporation, the Bishop Fox assessment team conducted a hybrid application assessment of the Acme application.

The assessment objective was to identify, within the designated time and scope, any security issues in the Acme application. The assessment team combined automated application vulnerability scanning, code review, and manual penetration testing techniques in order to rapidly locate attack vectors and simulate real world exploitation.

Acme has been provided the detailed findings and recommendations resulting from the assessment in an assessment report. At the time of this letter, the Bishop Fox assessment team has performed remediation testing.

Sincerely,

Vincent Liu
Partner
Bishop Fox

Letter of Assessment Type 4

8240 S. KYRENE ROAD
SUITE A-113
TEMPE, AZ 85284
UNITED STATES

WWW.BISHOPFOX.COM

February 31, 2050

Acme Corporation
10 Ton Parkway
Albuquerque, NM 12345
United States

To Whom It May Concern:

In February of 2050, pursuant to our agreement with Acme Corporation, the Bishop Fox assessment team conducted a hybrid application assessment of the Acme application.

The assessment objective was to identify, within the designated time and scope, any security issues in the Acme application. The assessment team combined automated application vulnerability scanning, code review, and manual penetration testing techniques in order to rapidly locate attack vectors and simulate real world exploitation.

Acme has been provided the detailed findings and recommendations resulting from the assessment in an assessment report, which includes one high-risk vulnerability (one instance), two medium-risk vulnerabilities (two instances), and three low-risk vulnerabilities (three instances). At the time of this letter, the team has performed remediation testing and confirms that all identified issues have been remediated.

Sincerely,

Vincent Liu
Partner
Bishop Fox