BISHOPFOX

WHAT TO EXPECT

GOOGLE PARTNER SECURITY ASSESSMENT

OUR PURPOSE:

TO SUPPORT PARTNER AND CUSTOMER SECURITY

The **Google Partner Program (GPP)** is a collaborative effort to protect partners, customers, and Google data by increasing the security of applications and networks that integrate with Google ecosystems.

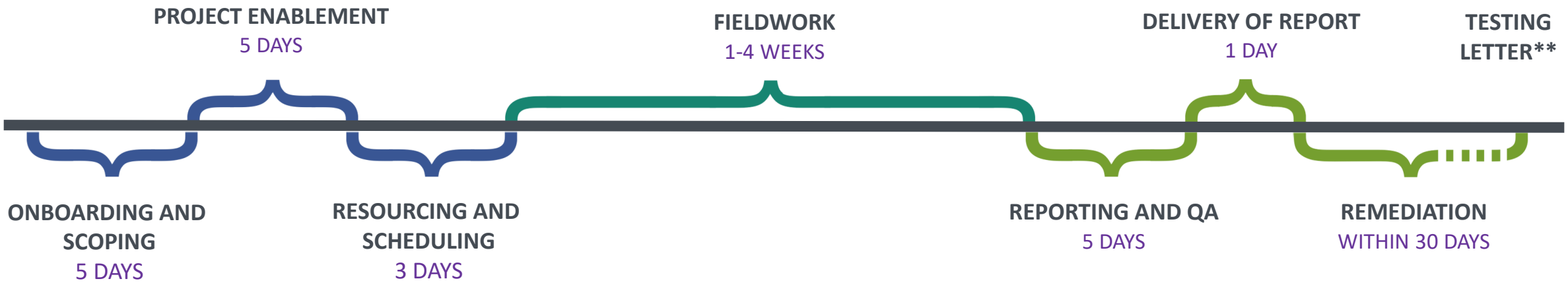
Google has engaged Bishop Fox to conduct testing with the goal of validating the security of Google partners' applications and **ensuring Google user data is handled securely.**

Bishop Fox's main goal is to help you complete the security assessment requirements for OAuth API Restricted scopes listed on the Google OAuth Application Verification FAQ.

PROJECT ACTIVITIES

PROJECT TIMELINE

Estimated timeline* based on average engagement size



Average GP Project Duration
(From contract signed to testing letter)

6-8 weeks, depending on scope and remediation period (if needed)

*Timelines can shorten if there is a quick turnaround on requested project enablement information

**Recertification partners have individual testing letter expirations and deadlines.

KEY POINTS

ONBOARDING AND SCOPING

ONBOARDING

You will be sent a **scoping survey** to collect initial details about your company and application (including your Google Project number). If you have questions or need assistance, a call can be scheduled with your Bishop Fox Account Manager.

Google Partners must **complete the application verification process with Google**. If you submitted an app that requests restricted scopes, and the app accesses Google user data from or through a server, one of the follow-up verification steps will be to get your app reviewed by an independent security assessor. Google OAuth Verification Requirements for additional details.

SCOPING SURVEY

BASIC INFORMATION

Primary Business Contact: Enter details here (e.g. Wile E. Coyote, wcoyote@acme.com, 555-5555)

Primary Technical Contact: Enter details here (e.g. Wile E. Coyote, wcoyote@acme.com, 555-5555)

Application Name: Enter name here (e.g. ACME Web Portal)

Components: ☐Web App ☐Gmail Add-on ☐Chrome Extension ☐Other: Enter text here

APIs used within application:
☐ Gmail ☐ Other (e.g., Nylas)

Third-party Hosting / Cloud Hosting: ☐ No ☐ Yes: Enter provider(s) here (e.g., AWS, Azure, Digital Ocean)

URL(s): Enter URLs here (e.g. http://portal.acme.com)

Has the application(s) passed Google's verification?
☐ Yes ☐ No

Google Project Number(s)*:

Do you have any blackout dates or timing requirements? Enter schedule constraints here (e.g. Complete testing before July 2050) Enter dates here

Are there any special access requirements (i.e. VPN required)? If so, please list: Enter details here

DETAILED APPLICATION INFORMATION

What is the primary use of the application? If there are multiple applications, please complete a separate survey for each application.

What programming languages, frameworks, databases, and other technologies are used to build the application?

What Gmail data is processed by your application?

How are application servers deployed / managed / updated?

KEY POINTS

ONBOARDING AND SCOPING

SCOPING

A Solutions Architect will use the completed scoping survey to determine the appropriate testing scope. The scope is based on the size and complexity of the application and environment, so it is important to **fill out the survey accurately** and **provide additional documentation where possible**.

All Google assessments include application penetration testing, external penetration testing, a cloud security review or host-based review, and a security assessment questionnaire (SAQ). ***Note:*** Please **exclude test code and third-party code** from the line of code count where possible. This helps prevent over-scoping.

NEXT STEPS

A Bishop Fox Account Manager will provide an estimated quote. Once pricing is agreed on, a **statement of work** (SOW) will be sent for your review. After signing, your account team will facilitate introductions to the engagement management team for collection of **Project Enablement**.

GETTING READY FOR THE ASSESSMENT

PROJECT ENABLEMENT

List of items typically needed to begin the assessment:

PROJECT ENABLEMENT REQUIREMENTS (Needed prior to project start)	**SECURITY ASSESSMENT QUESTIONNAIRE (SAQ)**	**EXTERNAL PENETRATION TESTING**	**APPLICATION PENETRATION TESTING**	**CLOUD SECURITY REVIEW***
URLs/IP addresses	N/A	**IP addresses in scope, along with registered domains and subdomains**	**Application URL**	N/A
Credentials/accounts	N/A	N/A	**3 test accounts per role**	**Cloud account assessor access**
Host environments confirmed	N/A	**Yes**	**Yes**	**Yes**
Documentation, diagrams, guides	**Completed SAQ form, Incident Response Plan, Information Classification and Handling Policy**	Optional: Network diagram or relevant external network documentation	Optional: Documentation on user functionality and documentation on APIs	N/A

*May be a host-based review if you do not use a cloud platform

RESOURCING AND SCHEDULING

RESOURCING AND SCHEDULING

Your Bishop Fox engagement management team works closely with the staffing and scheduling team to ensure the **best consulting resources for your needs** are allocated to your project (based on scope and testing types).

Once consulting resources are identified, the project schedule is planned and communicated to you and a **project kick-off meeting** is set. The exact order of testing (application, external, cloud, SAQ) will be based on the availability of your assigned project resources and expected duration of the individual testing activities. The engagement manager will communicate these specific dates during kick off.

If you have any **requests regarding the timing of the start of your assessment** (e.g., earliest available start date on your side), please notify your engagement management team to have that accounted for in our scheduling efforts.

FIELDWORK

FIELDWORK

Our testing approach is collaborative with Google partners. We will perform time-limited penetration testing to find as many potential security issues as possible, with a **focus on validating that the level of secure data handling established by Google is in place.**

All testing will be performed **remotely** unless an exception is granted and determined in advance.

During testing, the Bishop Fox team will provide, at a minimum, **weekly status updates** to your team. **Critical- and high-severity findings, as well as mandatory requirements missing (from the SAQ), will be reported within 24 hours**. Status updates will include completed tasks, preliminary findings, current activities, and planned activities.

WRAPPING UP THE ASSESSMENT

DELIVERABLES AND REMEDIATION TESTING

ASSESSMENT REPORT

The report includes an **executive summary** detailing a project overview, project scope, summary of findings, and strategic next steps. The **assessment section** includes a review of technical findings including vulnerability descriptions, severity levels, affected systems, technical impact, remediation recommendations, and walkthroughs of exploitation with screenshots if applicable.

REPORT WALKTHROUGH

Bishop Fox will walk through the report with the partner team and any relevant stakeholders. Walkthrough includes a **review of the project approach and scope, discussion of individual findings and recommendations, and guidance on next steps**.

REMEDIATION TESTING

Once the partner has remediated any vulnerabilities found during testing, Bishop Fox will **perform one round of remediation testing** to validate the issues are fully resolved.

Remediation must be requested after fieldwork has been completed and within 30 days of report delivery.

If additional rounds of remediation testing are needed, we can create a change order for the additional days of testing that are required.

TESTING LETTER

All testing letters will be issued at Bishop Fox's discretion and **submitted to Google by Bishop Fox**. See criteria for the testing letter on the next slide.

TESTING LETTER

CRITERIA, DETAILS, DATES

CRITERIA

Bishop Fox will author and issue a testing letter to Google if the following qualifications have been met:

- ☑ **For all partners: All critical- and high-severity vulnerabilities and mandatory requirements** from the SAQ reported from your assessment have been **verified as remediated**.
  - Retesting low-severity findings and informational issues for remediation is not required prior to issuance of a letter and is to be done at your discretion.

LETTER DETAILS

The letter includes an engagement overview, services or activities performed (i.e., reference to the Google testing requirements), testing dates, testing environment, list of testing targets, and your OAuth API Restricted scopes.

LETTER DATES

Google testing letter date will be date of issuance.

Testing letter is valid from date of issuance + 365 days

ANNUAL TESTING

RECERTIFICATION

RETURNING GOOGLE PARTNERS

In anticipation of your return, we have kept track of your **scoping information and project notes from your past assessment**. In order to accurately scope your reassessment, we ask that you complete a new scoping survey. This will allow us to compare last year's data with this year's data and scope out the amount of effort that will be needed for your upcoming project.

We are happy to assist if your assessment was completed by another Google-approved assessor. We may ask you to submit your report, under MNDA, along with your scoping survey. This will allow our team to review previous findings and accurately scope out the effort needed for your assessment.

ANNUAL TESTING EFFICIENCIES

Bishop Fox can rescope the partner testing environment following the same scoping process with the added benefit of prior data and testing notes.

Bishop Fox will **keep track of each partner's scoping information from year to year** and leverage this data when scoping subsequent testing projects. This has the benefit of potentially reducing effort required for follow-up testing.

Any relevant testing notes taken during the initial project will be archived by Bishop Fox for follow-up testing to **reduce ramp-up time for Bishop Fox consultants**.

Previously developed test harnesses or testing scenarios will be reused or repurposed to **improve testing efficiency**.

Additional FAQs: HTTPS://SERVICES.BISHOPFOX.COM/GOOGLE

FREQUENTLY ASKED QUESTIONS

- **HOW MUCH WILL THE ASSESSMENT COST?**

  We have negotiated discounted pricing with Google for this program, and the cost is between $15,000 - $75,000 depending on the size of the application, the size of the environment, and how Google customer data is used.

- **WHEN WILL THE ASSESSMENT START?**

  Partners will need to provide full project enablement items (e.g., credentials, test accounts, documentation) before receiving a start date. This is to ensure that there are no delays to the project schedule.

- **HOW LONG WILL THE ASSESSMENT TAKE?**

  Once all the paperwork is in place, fieldwork can typically take up to one-to-four weeks. After that, reporting and QA can take up to one week for assessment report delivery. This does not include remediation time.

- **WHAT WILL THE SCOPING INFORMATION BE USED FOR?**

  Information shared with us for scoping will be used to determine overall effort required and also to shorten the ramp-up time needed for testing. If we can understand the environment before testing, we can spend less time on discovery/footprinting and more time on active penetration testing. The more accurate the scoping details are, the more accurate and cost-sensitive we can be with the scope and quote.

- **ONLY A SMALL PART OF MY APPLICATION USES GOOGLE APIS. DOES IT ALL GET INCLUDED IN SCOPE?**

  Yes, unless Google customer data is clearly isolated from other parts of your application, we need to test the entire application. If an attacker can exploit one part of your application not directly related to Google, that exploit could be used to compromise Google customer data.

GET IN TOUCH **WITH US**

bishopfox.com/google

THANK **YOU**

PROJECT ACTIVITIES

EXTERNAL PENETRATION TESTING

APPROACH

- **Real-world attack simulation** focused on identification and exploitation
- **Discovery and enumeration** of live hosts, open ports, services, unpatched software, administration interfaces, authentication endpoints lacking MFA, and other external-facing assets
- Automated vulnerability scanning combined with **manual validation**
- **Brute-forcing** of authentication endpoints, directory listings, and other external assets
- Analysis of vulnerabilities to validate and develop complex **attack chaining** patterns and custom exploits
- **Exploitation of software** vulnerabilities, insecure configurations, and design flaws

SCOPE

- External, internet-facing infrastructure, systems, and relevant applications that interface with the Google ecosystem and/or handle sensitive customer data

PROJECT ACTIVITIES

APPLICATION PENETRATION TESTING

APPROACH

- **Real-world attack simulation** focused on identification and exploitation
- **Discovery of attack surface**, authorization bypass, and input validation issues
- Automated vulnerability scanning combined with **manual validation**
- **Exploitation** of software vulnerabilities, insecure configurations, design flaws, and weak authentication
- Analysis of vulnerabilities to validate and develop complex **attack chaining** patterns and custom exploits

SCOPE

- Partner applications that integrate with a Google ecosystem, especially applications that handle sensitive Google or customer data

PROJECT ACTIVITIES

CLOUD SECURITY REVIEW

APPROACH

- Gather all available cloud configuration **settings and metadata**
- Identify **gaps or deviations** from accepted cloud provider's security best practices

SCOPE

- Cloud environment for all partner infrastructure, systems, and relevant applications that interface with the Google ecosystem or handle sensitive customer data

PROJECT ACTIVITIES

SELF-ASSESSMENT QUESTIONNAIRE (SAQ)

APPROACH

- **Targeted questions** about how the partner organization addresses common threats, based on industry trend reports, CIS CSC Top 20, and Bishop Fox's experience
- Review of SAQ responses, rating responses as met, partially met, or not met based on **standardized evaluation criteria**

SCOPE

- Internal control environment for all partner infrastructure, systems, and relevant applications that interface with the Google ecosystem or handle sensitive customer data

PROJECT ACTIVITIES

REMEDIATION TESTING

APPROACH

- **Perform one round of remediation testing** against those issues identified by the partner as having been remediated
- Remediation testing to take place **after fieldwork is completed**; must be requested **within 30 days after report delivery**

SCOPE

- Vulnerabilities identified as part of the partner security testing program

NOTES

- Remediation testing can be separately scoped based on final report or built into the initial assessment scope. If additional rounds of remediation testing are needed, we can create a change order for the additional days of testing that are required.
- Remediation testing will be performed at the end of the assessment **once all required fixes** have been completed. This helps keep the assessment schedule on track and ensures fieldwork hours go towards completing the assessment work.