

Security Assessment

The objective of the Security Assessment is to help the customer's IT team improve the security posture of a Google domain by assessing current domain configuration, security processes, and procedures. This is followed by introducing new security tools and training for administrators and end users on security best practices.

Key Activities

Security Assessment

Audit existing G Suite security settings and policies against best practices, identifying potential risks.

Security Workshop

Half-day, on-site workshop to educate on the latest security field insights, discuss threats, and review the Security Assessment findings. Determine relative priority of recommended actions.

Implementation Plan Recommendations

Create an implementation plan checklist to address recommended initiatives, owners, risks, and blockers.

Response Plan Recommendations

Advise on the creation or update of an incident response plan based on Google's best practices.

Security Training Recommendations

Advise on training updates for new and existing employees to help meet desired security objectives.

Deliverables

Security Assessment, including:

- Implementation plan recommendations
- Response plan recommendations
- Security training recommendations

Scope and Pricing

- Up to five days engagement (on-site or off-site at Google's discretion) within one week period
- Maximum of ten participants in workshop
- Pricing will be agreed upon by customer and Google and specified in the applicable Ordering Document

Terms and Conditions: This datasheet is associated with the following SKU: GAPPS-PROF-SVC-SA. The services described in this datasheet are governed by the applicable fully signed Ordering Document and any incorporated terms and conditions.

© 2017 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

Rev: 03/2017-3