Statement of Work
Onapsis Health Check Service

The primary goal of the Professional Services hereunder is to assist Your security, compliance, and development teams understanding tactical and strategic methods to maximize the value You receive from Onapsis' Products to secure Your business-critical applications based on industry leading frameworks.

As part of an effective security program, we will help You with an independent evaluation of Your investment in Onapsis Products. Key benefits include measuring Your progress in addressing the most critical risks facing Your business-critical applications and enhancing related security capabilities and controls. This health check service helps illustrate gaps in key processes to enhance cross functional alignment between security, compliance, and development teams for the areas assessed. This independent evaluation helps InfoSec and governance teams identify gaps in controls and consider steps to mitigate the greatest risk.

1. Service Overview

The primary objective of this SOW is to evaluate Your use of Onapsis' Product(s) purchased once Your teams have become familiar with their deployment and established an operational cadence. An overview of the health check service for each Product is included in the below section entitled Professional Services Activities and Approach, but only those Professional Services by Product included in Your signed Order Form are applicable. The Onapsis project team will work with Your designated team members to execute the tasks described below.

2. Services Activities and Approach

The scope of the health check service is for the Products per the executed Order Form. The Professional Services will be subject to Section 9 - Service Package Assumptions identified below.

The Onapsis project team will support and assist You with the health check tasks:

- Confirm Your Participants
- Review approach
- Schedule sessions with You
- Prepare assessment, templates, questionnaire, and kick-off slides
- Brief health check participants and administer questionnaire with You
- Develop health check report
- Meet with You to present the report, review results, discuss leading practices, and path forward.

The applicable offering-specific activities below:

Assess	Assess & Comply	Defend	Control
• Collect vulnerability scan data and confirm responses	• Collect vulnerability scan data and code scan data and confirm responses	• Collect notable events and incident output	• Collect code scan data and confirm responses

• Validate responses with Assess output and analyze data • Analyze scan results	• Validate responses with Assess and Comply output and analyze data • Analyze scan and audit results	• Validate responses with notable Defend events and incidents output and analyze data • Analyze Defend results	• Validate responses with Control output and analyze data • Analyze code results using workbook template
PS-SV-HC-ASSESS-O	PS-SV-HC-ASSESSCOMP-O	PS-SV-HC-DEFEND-O	PS-SV-HC-CONTROL-O

3. Resource and Artifact Requirements

You agree to make the following resources and artifacts available for the success of this service without undue delay noted in the table below. Failure to provide resources and artifacts may result in a delay of the Professional Services. For the resources listed below, the role name and individual assignments may differ by organization, and we will work with You to confirm participants prior to kick-off of the Professional Services.

- Point of Contact / PM
- Application Administrator
- Application Security Specialist
- Information Security Manager

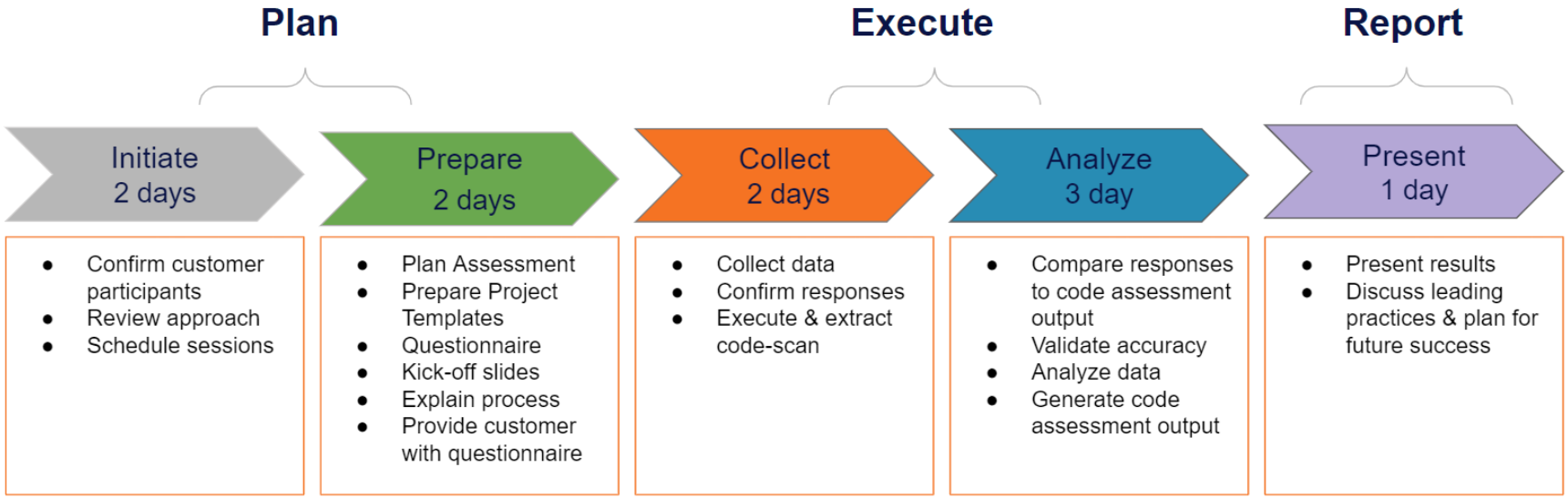
Assess	Assess & Comply	Defend	Control
Resources: • Compliance and Controls Specialist • Onapsis Product Administrator Artifacts: • Assessment Scan for all systems (XLSX) • Issues Extended Report showing accepted issues (XLSX) • Assets Extended Report (XLSX)	Resources: • Compliance and Controls Specialist • Onapsis Product Administrator Artifacts: • Comply Audit Scan for active policies • Issues Extended Report showing accepted issues (XLSX) • Assets Extended Report (XLSX)	Resources: • Security Operations Center (SOC) Manager • Incident Response Specialist • Onapsis Product Administrator Artifacts: • Defend Notable Events sorted by occurrence screenshot • Incidents sorted by occurrence screenshot • Incident Profile - Incident Summary Report • Issues Extended Report showing accepted issues (XLSX) • Assets Extended Report (XLSX)	Resources: • Secure Coding Specialist • Change Management Specialist • Development Team Lead • Quality Assurance Specialist Artifacts: • Inventory Analysis • SAP CP Export Report - findings output report • TP type data and report • Onapsis Control output review spreadsheet • Deprecated program list, last updated

4. Estimated Schedule

The delivery schedule for Professional Services will be 2 to 3 weeks from project kick-off and shall be performed in a timely and professional manner. Onapsis will work with You to coordinate a project start and align on required resources.

5. Methodology

The Onapsis project team will utilize the following methodology for Professional Services delivery:



Health Check Bootcamp Session - Focus on Control - DRAFT.pptx

6. Deliverables

The Professional Services include the following deliverables (the "**Deliverables**"). Onapsis will provide documentation related to Deliverables to You in electronic format as outlined in the table below.

Deliverables	Description
Survey Results	Report showing Your responses.
Conclusions and recommendations	Responses relative to survey results and Onapsis product outputs. Recommendations made to improve overall Onapsis product effectiveness and align with leading security and coding practices.
Output Analysis	Onapsis reports will be reviewed and analyzed.

7. Completion Criteria

These Professional Services shall be deemed complete upon one the following criteria:

- Completion of all Deliverables detailed herein; or
- After three (3) weeks from project kick-off or twelve (12) months from purchase date. In the event an extension of time is required, the parties will sign a Change Order.

8. Out of Scope

The following items are identified as out-of-scope for the Professional Services:

- Assessment of non-licensed systems.
- Assessment of systems third party systems that interact with Onapsis-supported platforms.
- Configuration of the Onapsis Platform or connected systems.

9. Service Package Assumptions

- You are responsible for ensuring the Onapsis Products are functioning and can perform the requisite tasks to provide the needed artifacts for performing the Professional Services.
- You are responsible for overall Project Management and Your resources being available: Onapsis and Your designated team member shall work closely together to ensure that the project scope remains consistent, and issues are resolved on a timely basis.

10. Terms and Conditions

This SOW is for project informational purposes only. Onapsis makes no warranties, expressed or implied in this SOW. Unless otherwise agreed between the parties, all Professional Services engagements are governed by the Onapsis Professional Services Terms and Conditions found here https://onapsis.com/legal.