Service Description: Cisco Security Optimization Service

This document describes Cisco Security Optimization Service.

Related Documents: This document should be read in conjunction with the following documents also posted at www.cisco.com/go/servicedescriptions/: (1) Glossary of Terms; (2) List of Services Not Covered; and (3) Severity and Escalation Guidelines. All capitalized terms in this description have the meaning ascribed to them in the Glossary of Terms.

Direct Sale from Cisco. If you have purchased these Services directly from Cisco, this document is incorporated into your Master Services Agreement (MSA) with Cisco. In the event of a conflict between this Service Description and your MSA, this Service Description shall govern.

Sale via Cisco-Authorized Reseller. If you have purchased these Services through a Cisco-Authorized Reseller, this document is for description purposes only; is not a contract between you and Cisco. The contract, if any, governing the provision of this Service will be the one between you and your Cisco Authorized Reseller. Your Cisco Authorized Reseller should provide this document to you, or you can obtain a copy of this and other Cisco service descriptions at www.cisco.com/go/servicedescriptions/.

Service Summary

The Cisco Security Optimization Service is intended to supplement a current support agreement for Cisco products. Cisco shall provide the Security Optimization Service described below as selected and detailed on the Purchase Order for which Cisco has been paid the appropriate fee. Cisco shall provide a Quote for Services (“Quote”), identifying the various service elemnts with the coresponding SKUs as shown in Appendix A, setting out the extent of the Services and duration that Cisco shall provide such Services. Cisco shall receive a Purchase Order that references the Quote agreed upon between the parties and that, additionally, acknowledges and agrees to the terms contained therein.

General Service Responsibilities

Cisco and the Customer shall have general responsibilities found in this section below.

General Service Responsibilities of Cisco

Cisco shall provide the following General Service provisions for any Security Optimization Service specified in the Quote:

- Under this Service, Cisco shall provide the Security Optimization Service during Standard Business Hours, unless stated otherwise.
- Provide a single point of contact ("Cisco Project Manager") for all issues relating to the Services.
- Participate in regularly scheduled meetings with the Customer to discuss the status of the Services.
- Ensure Cisco employees (including Cisco subcontractors) conform to Customer’s reasonable workplace policies, conditions and safety regulations that are consistent with Cisco’s obligations herein and that are provided to Cisco in writing prior to commencement of the Services; provided, however, that Cisco’s personnel or subcontractors shall not be required to sign individual agreements with Customer or waive any personal rights.
- Supply Cisco project team personnel with a displayable form of identification to be worn at all times during services activities at Customer’s facility.
- Cisco reserves the right to determine which of its personnel shall be assigned to a particular project, to replace or reassign such personnel and/or subcontract to qualified third persons part or all of the performance of any Security Optimization Service hereunder. Should Customer request the removal or reassignment of any Cisco personnel at any time; however Customer shall

be responsible for extra costs relating to such removal or reassignment of Cisco personnel. Cisco shall not have any liability for any costs, which may occur due to project delays due to such removal or reassignment of Cisco personnel.

General Responsibilities of Customer

General Services

Customer shall comply with the following obligations for General Services for any Security Optimization Service specified in the Quote:

- Designate at least two (2) but not more than six (6) technical representatives, who must be Customer's employees in a security engineer or administrator role, to act as the primary technical interface to the Cisco designated engineer(s). Customer will designate as contacts senior engineers with the authority to make any necessary changes to the Network configuration. One individual, who is a senior member of management or technical staff, will be designated as Customer's primary point of contact to manage the implementation of services under this Service Description (e.g., chair the weekly conference calls, assist with prioritization of projects and activities).
- Ensure key engineering, networking and operational personnel are available to participate in interview sessions and review reports as required by Cisco in support of Service.
- Customer's technical assistance center shall maintain centralized network and security management for its Network supported under this Service Description, capable of providing Level 1 and Level 2 support.
- Provide reasonable electronic access to Customer's Network to allow the Cisco designated engineer to provide support.
- Customer agrees to make its production, and if applicable, test Network environment available for installation of Data Collection Tools. Customer shall ensure that Cisco has all relevant Product information needed for an assessment.
- If Cisco provides Data Collection Tools or scripts located at Customer's site, Customer shall ensure that such Data Collection Tools or scripts are located in a secure area, within a Network environment protected within a firewall and on a secure LAN, under lock and key and with access restricted to those Customer employee(s) or contractor(s) who have a need to access the Data Collection Tools and/or a need to know the contents of the output of Data Collection Tools. In the event Data Collection Tool provided by Cisco is Software, Customer agrees to make appropriate computers available and download Software as needed. Customer shall remain responsible for any damage to or loss or theft of the Data Collection Tools while in Customer's custody.
- Provide a Network topology map, configuration information, and information of new features being implemented as needed.
- Provide requirements documentation, low-level and high- level designs, implementations plans, and test plans as required for specific services.
- Notify Cisco immediately of any major security policy (e.g. firewall rule change; Cisco ISE policy change) or Network changes (e.g. topology; configuration; new IOS releases; moves, adds, changes and deletes of devices).
- In the event the Network or Security composition is altered, after this Service Description is in effect, Customer is responsible to notify Cisco in writing within ten days (10) of the change. Cisco may require modifications to the fee if the Network composition has increased beyond the original pricing quote for Services.
- Create and manage an internal email alias for communication with Cisco.
- Retain overall responsibility for any business process impact and any process change implementations.
- Supply the workplace policies, conditions and environment in effect at the Customer's facility.
- Provide proper security clearances and/or escorts as required to access the Customer's facility.
- Customer agrees that it will not hire a current or former employee of Cisco, who is involved in the Services under this Service Description, during the term of the Service and for a period of one (1) year after the termination of the Service. As liquidated damages, and not as a penalty, should Customer hire a current or former Cisco employee who is involved in the Services under this Service Description, Customer shall pay to Cisco three (3) times the annual compensation of such employee on the date the employee is hired. If payment is not made on such date, the liquidated damage payment shall be six (6) times the annual compensation of such employee.

In addition to the General Responsibilities, Cisco and the Customer each shall comply with obligations as required for Integration (CON-AS-SEC) and Advisory (CON-AS-SECADV) security services shown below.

Specific Integration Service Details (CON-AS-SEC)

This section provides the service details for the following Integration services:

- Network Device Security Assessment (NDSA)
- Security Advanced Change Support (Security Advanced CS)
- Security Change Support (Security CS)
- Security Cyber Range (Security CR3)
- Security Cyber Range (Security CR5)
- Security Design Development Support (Security DDS)
- Security Design Review and Support (Security DRS)
- Security Health Check (Security HC)
- Security Issue Resolution and Planning Support (Security IRPS)
- Security Kick-Start Support (SKSS)
- Security Knowledge Service (Security KS)
- Security Network Consulting Support (Security NCS)
- Security Ongoing Flexible Support (Security OFS)
- Security Performance Tuning Support (Security PTS)
- Security Proactive Software Recommendations (Security PSR)
- Security Remote Knowledge Transfer (Security RKT)
- Security Strategy and Planning Support (SSPS)
- Security Technology Readiness Assessment (STRA)
- Security Validation and Testing Premier Support (Security VTPS)
- Security Validation and Testing Support (Security VTS)
- Software Security Alert (SSA)

Network Device Security Assessment

Specific Service Responsibilities of Cisco

Cisco will consult with the Customer to provide a review of the NDSA service, answer questions, and establish mutually-agreed upon expectations for the scope of the assessment and the level of device configuration sampling. Network Device Security Assessment may include, among other information, the following:

- Assess up to 350 Cisco device configurations, but only 10 of those devices may be firewalls.
- Review of Customer's device security templates.
- Provide an encrypted method for the customer to provide device configurations and policies.
- Analyze device configurations focused on configuration security hardening of the individual devices.
- Analyze firewall rules for common configuration issues.
- Provide secure encrypted delivery of the Assessment Report, which will include: Gap assessment comparing Customer's current practices to Cisco's recommended best practices, and Prioritized list of discovered vulnerabilities and most critical findings.
- An interactive presentation of findings, analysis, and recommendations.
- The deletion, removal, and destruction of collected customer data (device list, device configurations, and device policies) from Cisco repositories.
- The deletion, removal, and destruction of all draft versions of the assessment report.

Specific Service Responsibilities of the Customer

Customer agrees to provide individuals with appropriate expertise and information about the network devices to meet with Cisco to provide information on the Customer desired goals and outcomes of the assessment, and insights into relevant business and technical requirements. Once the specialized assessment team has started analyzing configurations, the device list and configurations may not be changed. Customer is responsible for the following:

- Provide a list of up to 350 devices, of which 10 may be firewalls, to be included in the assessment.
- Supply all listed device configurations and versions in a secure, encrypted manner.
- Ensure all device configurations and versions are accurate and up-to-date.
- Confirm that configurations submitted match the Customer device list.
- Ensure all relevant Customer stakeholders attend the Cisco interactive presentation of findings, analysis, and recommendations.
- Review and submit comments and requests for changes within 10 business-days of the Cisco interactive presentation of findings, analysis, and recommendations.
- Request in writing by an authorized person, the destruction of the finalized assessment from Cisco repositories.

Security Advanced Change Support

Specific Service Responsibilities of Cisco

Security Advanced Change Support consists of a Cisco Security Consulting Engineer to support design of Customer plans (network drawings, implementation plan, test plan rollback plan), and configuration changes (device configurations and cabling changes).

Emergency Changes. Cisco's ability to support an emergency change is dependent on availability of resource. Cisco has no obligation to support an emergency change if Cisco is unable to assign a Cisco Security Consulting Engineer to support the change.

Planned Changes. For planned changes (scheduled twenty-one (21) calendar days in advance), Cisco will have a Cisco Security Consulting Engineer assigned.

During the change window, the Cisco Security Consulting Engineer will observe, provide input and feedback, and will engage directly when authorized. In the case of a rollback, the Cisco Security Consulting Engineer will support de-briefing activities, lessons-learned, and moving forward planning. The Cisco Security Consulting Engineer will support post-change efforts to validate stability and operational functionality. Other Cisco responsibilities include:

- Plan Development and review of existing plans (e.g., network drawings, implementation plan, test plan, rollback plan).
- Review with Customer for input, recommendations and feedback on plans.
- Plan Development and review of planned changes (e.g., device configurations, cabling changes).
- Provide Change Plan and Device Configurations Report.
- Change Support Window (e.g., troubleshooting support, implementation support, support relevant Customer opened TAC cases).
- Post- Change Implementation Support (e.g., troubleshooting support, performance review, stabilization efforts).

Limitations:

- Changes may not include more than two (2) security devices or two (2) pairs of security devices (e.g., active-standby firewall pairs).
- Changes may not include more than ten (10) network devices.
- Cisco will determine the content and format of the deliverable.
- A change support window may not be longer than eight (8) hours. There may be no more than two (2) change support windows. Change support windows may be after Standard Business Hours.

Specific Service Responsibilities of the Customer

Customer responsibilities include:

- Designate person(s) from within its technical support organization to serve as a liaison to the Cisco designated engineer.
- Provide its designated person(s) with instructions on process and procedure to engage the Cisco designated engineer.
- Provide Schedule, Change Window Information, change control process, escalation process, standard operating procedures, relevant nomenclature, and any other known, relevant constraints.
- Support development and review change plans (e.g., network drawings, implementation plan, test plan, rollback plan) with Cisco designated engineer.
- Provide recommendations and feedback on plans; provide explicit acceptance and rejections of recommendations.
- Support development and review planned changes (e.g., device configurations, cabling changes) with Cisco security engineer.
- Provide recommendations and feedback on planned changes; provide explicit acceptance and rejections of recommendations.
- Provide reasonable electronic access to Customer's Network and security devices to enable Cisco in providing support.
- Customer is responsible for migrating any content to a Customer template or any customizations.
- Customer is responsible for any Customer-specific forms, documents, scheduling responsibilities, Customer internal processes, etc.
- Customer is responsible for opening any cases with vendor's technical assistance center during change window (e.g. Cisco TAC)
- Customer is responsible for making configuration changes to devices.

Security Change Support

Specific Service Responsibilities of Cisco

Under Security Change Support (Security CS), Cisco will provide a Cisco designated engineer available during scheduled (planned or emergency) changes to the network, security devices, and security policies for the production environments.

Emergency Changes. Cisco's ability to support an emergency change is dependent on availability of resource. Cisco has no obligation to support an emergency change if Cisco is unable to assign a Cisco designated engineer to support the change.

Planned Changes. For planned changes (scheduled twenty-one (21) calendar days in advance), Cisco will have a Cisco designated engineer assigned.

During the change window, the Cisco designated engineer will observe, as the plan is executed, provide recommendations and feedback as needed, and will engage directly when authorized. In the case of a rollback, the Cisco designated engineer will support de-briefing activities, lessons-learned, and moving forward planning. The Cisco designated engineer will support post-implementation efforts to check the stability and operational functionality. The activities associated with this service should not exceed a period of seven (7) calendar days and will include the following:

- Review of Customer plans (e.g., network drawings, implementation plan, test plan, rollback plan).
- Provide recommendations and feedback on Customer plans.
- Reviewing Customer planned changes (e.g., device configurations, cabling changes).
- Provide recommendations and feedback on Customer planned changes.
- Change Window Support (e.g., troubleshooting support, implementation support, support relevant Customer opened TAC cases).
- Support of Post-Implementation Plan (e.g., troubleshooting support, performance review, stabilization efforts).

Reactive Support: Security Change Support is intended for planned changes. However, Customers may leverage/apply entitlement for this service for reactive situations that are unrelated to planned changes. In these instances, Cisco would provide the following:

- Provide technical evaluation of initial TAC problem diagnosis based on knowledge of Customer's network,
- Provide technical evaluation of proposed unscheduled change to Network, and,
- Provide technical representation in regularly scheduled conference calls.

For reactive situations (e.g., device failure, network outage), Customer may leverage the Security Change Support service for lifeline support; however, the following conditions apply:

- Customer must open a service request with the vendor's technical assistance center (e.g. Cisco TAC) prior to requesting support under Security Change Support.
- Entitlement for 1 unit of change support may not exceed forty (40) hours of support.
- Entitlement for 1 unit of change support may not exceed seven (7) calendar days.
- Root cause analysis is explicitly excluded; the Security Issue Resolution and Planning Support offers support for root cause analysis.

Limitations:

- A change support window may not be longer than eight (8) hours. There may be no more than two (2) change support windows. Change support windows may be after Standard Business Hours.

Specific Service Responsibilities of the Customer

Customer responsibilities include:

- Designate person(s) from within its technical support organization to serve as a liaison to the Cisco designated engineer.
- Provide its designated person(s) with instructions on process and procedure to engage the Cisco designated engineer.
- Provide Schedule, Change Window Information, change control process, escalation process, standard operating procedures, relevant nomenclature, and any other known, relevant constraints.
- Provide and Review Customer changes plans (e.g., network drawings, implementation plan, test plan, rollback plan) with Cisco security engineer.
- Consider Cisco's recommendations and feedback on Customer plans; provide explicit acceptance and rejections of recommendations.
- Provide Customer planned changes (e.g., device configurations, cabling changes) with Cisco security engineer.
- Consider recommendations and feedback on Customer planned changes; provide explicit acceptance and rejections of recommendations.

- Provide reasonable electronic access to Customer's Network and security devices to enable Cisco in providing support.
- Making configuration changes to devices.

For **Reactive Support** (e.g., device failure, network outage) unrelated to planned changes, Customers may leverage entitlement for Security Change Support to request assistance. Customer responsibilities in such cases include:

- Opening a service request with the vendor's technical assistance center (e.g. Cisco TAC) prior to requesting entitlement for reactive support.
- Ensure that Cisco security engineer has access to TAC case and notes, if non-Cisco TAC.
- Ensure that Cisco security engineer is included on all calls and discussions with TAC.
- Review with Cisco security engineer any proposed changes.

Security Cyber Range Small

Specific Service Responsibilities of Cisco

Under Security Cyber Range, Cisco provides a specialized technical training workshop to help security staff build the skills and experience necessary to combat modern cyber threats. Cisco activities may include:

- Provide Customer with workshop requirements.
- Provide Customer with workshop agenda.
- Conduct Cyber Range workshop.
- Provide standard Cyber Range workshop environment housed at a Cisco lab via remote VPN.
- Provide workshop attendees with workshop Attendance Certificate.
- Provide workshop attendees with a Service Completion Certificate.

Limitations:

- Workshops are limited to twelve (12) attendees.
- Workshops are limited to three (3) days on-site at a single Customer location during Standard Business Hours excluding Cisco holidays, locally recognized country holidays, vacations and training days, or if both Customer and Cisco agree, the workshop may be held at a designated Cisco location.

Specific Service Responsibilities of the Customer

Customer responsibilities include:

- Designate a single point of contact for all Cisco communication. This person has the authority to act on all aspects of the service being performed.
- Designate a backup contact when Customer contact is unavailable. This person has the authority to act on all aspects of the service in absence of the primary contact.
- Provide reasonable access to Customer site and facilities including, where applicable, computer equipment, telecom equipment, facilities and workspace. Customer shall provide proper security clearance and/or escorts as required to access equipment and/or lab facilities etc.
- Ensures that contracts with its own vendors, end users, and third parties are fully executed and reflect the correct terms to enable service delivery.
- Customer is responsible for the management, support, and direction of the resource supplied to Customer by Cisco.
- Provide Cisco with a connection to the Internet to access the Cyber Range workshop environment housed at a Cisco lab if the workshop is conducted at Customer site.
- Customer confirms workshop requirements are fulfilled two (2) weeks prior to workshop.
- Provide list of up to twelve (12) workshop attendee names.
- Attend Cyber Range Workshop at scheduled times.

Security Cyber Range Large

Specific Service Responsibilities of Cisco

Under Security Cyber Range, Cisco provides a specialized technical training workshop to help security staff build the skills and experience necessary to combat modern cyber threats. Cisco activities may include:

- Provide Customer with workshop requirements.
- Provide Customer with workshop agenda.
- Conduct Cyber Range workshop.
- Provide standard Cyber Range workshop environment housed at a Cisco lab via remote VPN.
- Provide workshop attendees with workshop Attendance Certificate.
- Provide workshop attendees with a Service Completion Certificate.

Limitations:

- Workshops are limited to twelve (12) attendees.
- Workshops are limited to five (5) days on-site at a single Customer location during Standard Business Hours excluding Cisco holidays, locally recognized country holidays, vacations and training days, or if both Customer and Cisco agree, the workshop may be held at a designated Cisco location.

Specific Service Responsibilities of the Customer

Customer responsibilities include:

- Designate a single point of contact for all Cisco communication. This person has the authority to act on all aspects of the service being performed.
- Designate a backup contact when Customer contact is unavailable. This person has the authority to act on all aspects of the service in absence of the primary contact.
- Provide reasonable access to Customer site and facilities including, where applicable, computer equipment, telecom equipment, facilities and workspace. Customer shall provide proper security clearance and/or escorts as required to access equipment and/or lab facilities etc.
- Ensures that contracts with its own vendors, end users, and third parties are fully executed and reflect the correct terms to enable service delivery.
- Customer is responsible for the management, support, and direction of the resource supplied to Customer by Cisco.
- Provide Cisco with a connection to the Internet to access the Cyber Range workshop environment housed at a Cisco lab if the workshop is conducted at Customer site.
- Customer confirms workshop requirements are fulfilled two (2) weeks prior to workshop.
- Provide list of up to twelve (12) workshop attendee names.
- Attend Cyber Range Workshop at scheduled times.

Security Design Development Support

Specific Service Responsibilities of Cisco

Cisco responsibilities under Security Design Development Support are limited up to one (1) complex solution set (e.g., Cisco ISE, Cisco Secure ACS, 802.1x deployments) or one (1) non-complex solution set up to forty (40) devices and include the following:

- Provide a Design Development Questionnaire
- Assist with or create Customer Requirements Document, as identified in the Quote
- Review Customer's requirements documentation and re-validate the requirements with Customer.
- Assist with either the High-Level Design Document or the Low-Level Design Document.

Specific Service Responsibilities of the Customer

Customer responsibilities include:

- Provide a completed Design Development Questionnaire, which will capture information such as the existing network infrastructure design, existing security infrastructure designs, planned designs, further growth requirements and additional customer requirements.
- Provide either the low-level or high-level design document describing the specific set of technical requirements and design goals and specifying the resulting Customer Network architecture and build-out plans to meet those requirements. The level of details must be sufficient to be used as input to an implementation plan.
- Provide or extract additional information required in the design effort (e.g., current and planned traffic characteristics).
- Provide documentation of any business requirements and technical requirements for the new design.
- Ensure all relevant customer stakeholders attend the Cisco interactive presentation of the Design Document recommendations.
- Review and submit comments and requests for revisions within 10 business-days of the Cisco interactive presentation of the Design Document.

Security Design Review and Support

Specific Service Responsibilities of Cisco

Cisco will consult with Customer via a series of remote meeting, up to 40 hours of support, to develop a thorough understanding of Customer's security design requirements and will perform the following:

- Review of Customer's design requirements, priorities, and goals.
- Review of security architecture and topology.
- Address design related questions.
- Analysis of impact of new requirements on existing network.
- Review and support of protocol design, selection and configuration.

- Review and support of feature design, selection and configuration.
- Review of device security considerations.
- Informal recommendations or advice about a security design.
- Help Customer resolve minor design-related issues

Specific Service Responsibilities of the Customer

Customer responsibilities include:

- Provide the low level design document describing the specific set of technical requirements and design goals specifying the resulting Customer Network architecture and build-out plans to meet those requirements. The level of details must be sufficient to be used as input to an implementation plan.
- Ensure key detailed design stakeholders and decision-makers are available to participate during the course of the Service.
- Provide or extract additional information required in the design effort (e.g., current and planned traffic characteristics).
- Provide documentation of any business requirements and technical requirements for the new design.
- Provide information on any current and planned traffic characteristics or constraints.

Security Health Check

Specific Service Responsibilities of Cisco

Cisco will perform a Security Health Check, limited to up to one (1) solution set or one (1) complex system (e.g., Cisco ISE, Cisco Secure ACS, 802.1x deployments) and up to twenty (20) devices responsibilities. Responsibilities will include:

- Review Customer's Security Health Check Request Questionnaire.
- Establish health check requirements, strategies, and schedules with Customer.
- Analyze configuration and policy implementations and align them with corporate security policies and procedures, and Cisco best practices,
- Analyze security devices.
- Recommend tuning changes to policy and devices configurations.
- Recommend design or architecture reviews, if needed.
- Identify relevant under-utilized product and solution capabilities.
- Conduct an Informal Knowledge Transfer on identified, relevant under-utilized capabilities (up to 2 hours in duration).
- Perform one (1) interactive tuning session with Customer to implement tuning recommendations.
- Provide a Security Health Check Report

Limitations:

- Performance tuning may be after Standard Business Hours.

Specific Service Responsibilities of the Customer

Customer responsibilities include:

- Complete the Security Health Check Request Questionnaire.
- Review completed Security Health Check Request Questionnaire with Cisco.
- Establish health check requirements, strategies, and schedule with Cisco.
- Provide electronic access to Cisco to devices such that analysis and tuning may be completed.
- Review and authorize Cisco's recommendations for tuning.
- Change management and scheduling of performance tuning.
- Assisting with interactive tuning session with Cisco to implement tuning recommendations.

Security Issue Resolution and Planning Support

Specific Service Responsibilities of Cisco

Cisco will review the security issues, identify the cause, and test and validate to confirm the issues have been identified with a proposed plan to address the issues. Cisco responsibilities include:

- Collect all relevant information regarding the issue.
- Analyze information.
- Review of Customer's device security goals and requirements.
- Provide secure, encrypted method for the Customer to provide device configurations and policies.

- Interactive presentation of findings, analysis, and recommendations.

Limitations:
Given the variety of situations and issues that may be encountered in production environments, issues may require a variety of services to compliment this service. For example:
- Security VTS or Security VTPS may be required to test and confirm causes in a lab environment.
- Design-related issues may require design-related services to produce a viable plan.
- Security IRPS provide insight in causes and a plan for resolving; however, executing the plan may require follow-on services.

Other limitations include:
- There is no guarantee that the root-cause analysis will result in a root-cause being identified or confirmed.
- Reasonable efforts will be made to provide conclusive findings and an issue resolution plan. Regardless, entitlement of an appropriate number of service units will be retired. For example, after a reasonable effort, including a Security VTPS lab re-create, to deduce the root-cause failure of one (1) security device that results in no-problem found, entitlement to one (1) unit of Security IRPS and one (1) unit of Security VTPS will be retired.
- Cisco Services may have to defer to product development engineering.
- Work may occur after Standard Business Hours.

Each unit of Security IRPS includes:
- Up to one (1) root-cause analysis; although, there may be multiple contributing causes.
- Up to six (6) security and/or network devices.
- Limited up to 80 hours.

Specific Service Responsibilities of the Customer

Customer responsibilities include:
- Supply all listed device configurations and versions in a secure, encrypted manner.
- Ensure all device configurations and versions are accurate and up-to-date.
- Ensure all relevant customer stakeholders attend the Cisco interactive presentation of findings, analysis, and recommendations.
- Designate person(s) from within its technical support organization to serve as a liaison to the Cisco designated engineer.
- Provide reasonable electronic access to Customer's Network and security devices to enable Cisco in providing support.
- Open any necessary cases with vendor's technical assistance center (e.g. Cisco TAC).

Security Kick-Start Support

Kick-Start Support is generally initiated following the completion of a Security Health Check where Cisco has identified product or solution capabilities that the Customer may be under-utilizing. Cisco will consult with the Customer to establish a plan and schedule for the Security Remote Knowledge Transfer, Security Design Review and Support, Security Change Support, and Security Performance Tuning further defined in this Service Description.

Security Knowledge Service

Specific Service Responsibilities of Cisco

Cisco will provide Security Knowledge Service, through a secure web-based portal ("Portal"). In addition to the security product and technology knowledge services included in this service, the Customer will also be provided with access to the foundational Network Infrastructure Modular Knowledge Service at no additional charge. Cisco responsibilities include:
- Customer user account creation for the Portal.
- Assist with getting the Security Knowledge Service operational with appropriate authentication and authorizations for user community.
- Release security content to the registered number of authorized viewers.
- Security content may be white papers, case studies, design guides, configuration guides, troubleshooting guides, training documents, deployment guides, or online books and/or manuals.
- Archive Customer-specific deliverables when delivered as part of an Advanced Services subscription engagement.
- Update Security content as Cisco may revise, update, and/or remove previously-released multimedia clips and/or content.

Specific Service Responsibilities of the Customer

Customer responsibilities include:

- Designate person(s) to be responsible for management of portal accounts within user community.
- Provide list of initial set of users to be authorized on the portal.

Security Network Consulting Support

Where available, Cisco will provide Network Consulting Support in the form of a designated engineer ("Advanced Services Engineer") to act as the primary interface with Customer, providing general advice and guidance related to Customer's Network, assessment recommendations, and remediation plans, up to five days per week (pending local work restrictions) during Standard Business Hours excluding Cisco holidays, locally recognized country holidays, vacation, and training days. Customer directed tasks to be performed by the Advanced Services Engineer are subject to Cisco approval, which shall not be unreasonably withheld..

Specific Service Responsibilities of the Customer

Customer responsibilities include:

- Provide Cisco with direction of activities and projects on which the Customer needs the Cisco engineer to engage.

Security Ongoing Flexible Support

Cisco will provide informal, Ongoing Flexible Support for incremental changes to the network security architecture. This flexible support may be applied to other work items within Security Optimization Service and 1 Unit is limited to 40 hours of assigned engineer's time. Cisco engineers will be assigned as work items are selected throughout the term of the service contract.

Specific Service Responsibilities of the Customer

Customer responsibilities include:

- Provide Cisco with details around what type of support is needed when a request is made.

Security Performance Tuning Support

Specific Service Responsibilities of Cisco

Cisco will provide Security Performance Tuning Support, consisting of the following:

- Meet with Customer to review Security Performance Tuning Support Questionnaire.
- Meet with Customer to establish performance tuning requirements, strategies, and schedule.
- Analyze configuration and policy implementations and align them with corporate security policies and procedures, and Cisco best practices,
- Analyze security devices.
- Recommend tuning changes to policy and devices configurations.
- Recommend design or architecture reviews, if needed.
- Perform one (1) interactive tuning session with Customer to implement tuning recommendations.
- Provide an informal (email) summary of key findings, tuning recommendations, and tuning performed. An additional unit of Security Performance Tuning Support will be charged to the Customer in the event formal documentation is requested.

Limitations:

Security Performance Tuning Support is not intended for complex-systems and solutions, such as:

- Cisco ISE environments
- Cisco Secure ACS deployments
- Network devices supporting complex 802.1x deployments

Each unit of Security Performance Tuning and Support includes:

- Up to one (1) solution set (e.g. firewall solution, VPN solution, intrusion prevention system) OR up to one (1) security device type (e.g. multi-purpose security devices supporting firewall, VPN, and IPS.
- For solution sets: Up to five (5) devices within given solution set for the first Security PTS unit.
- For solution sets: Up to five (5) additional devices for additional Security PTS units IF a new solution set is added. For example, if the Security PTS includes firewall and VPN solutions then two Security PTS units allows up to ten (10) firewall and/or VPN devices to be analyzed and tuned.
- For solution sets: Up to fifteen (15) additional devices for additional Security PTS units IF the solution set does not change. For

example, if the Security PTS includes a VPN solution then two Security PTS units allows up to twenty (20) VPN devices to be analyzed and tuned.

- For security device type: up to two (2) security devices.
- Work may occur after Standard Business Hours.

Specific Service Responsibilities of the Customer

Customer is responsible for the following:

- Complete the Security Performance Tuning Support Questionnaire.
- Meet with Cisco to review Security Performance Tuning Support Request Form
- Meet with Cisco to establish performance tuning requirements, strategies, and schedule.
- Provide electronic access to Cisco to devices such that analysis and tuning may be completed.
- Reviewing and authorizing Cisco's recommendations for tuning.
- Change management and scheduling of performance tuning.
- Assisting with interactive tuning session with Cisco to implement tuning recommendations.

Security Proactive Software Recommendations

Specific Service Responsibilities of Cisco

Cisco will provide proactive software recommendations that evaluate the various Security Software versions against internal Cisco caveat databases. Cisco will be responsible for the following:

- Provide the Security PSR Questionnaire.
- Gather Customer provided Security Software information, feature, functionality and capability requirements.
- Review the new Security Software features requested by the Customer.
- Document all features to be included in the Security Software Recommendation
- Evaluate the installed Software releases and new versions for interoperability issues and the ability to support current and future business and technical requirements.
- Provide detailed report including known caveats to which Customer may be exposed and if possible, appropriate workarounds for current and future business and technical objectives.

Limitations:

Each unit of the Security Proactive Software Recommendation includes:

- Up to one (1) software recommendation for one (1) Cisco product.
- Up to three (3) feature set profiles, based on up to five (5) sample configurations for each profile, provided by customer as representatives of deployed products.

Specific Service Responsibilities of the Customer

Customer is responsible for the following:

- Complete the Security PSR questionnaire.
- Provide Cisco with sample configurations for the Software being reviewed.
- Provide Cisco with a network diagram showing the devices and their relationship to other equipment in the Customer network.
- Provide Cisco with a list of required new features that need to be supported by the software to be reviewed.
- Review and accept the list of features to be included in the recommendation as provide by Cisco.
- Review and approve the recommendation results if it meets all requirements of the Customer.

Security Remote Knowledge Transfer

Specific Service Responsibilities of Cisco

Cisco will consult with Customer to identify requirements and topics for informal training sessions. Remote Knowledge Transfer Sessions are:

- Delivered in English (other languages subject to availability),
- Delivered remotely for up to four (4) hours in length, with no labs and no printed course materials,
- Relevant to the Cisco products and technologies deployed in Customer's production Network.
- Formal knowledge transfer sessions focusing on best practices for operating, tuning, maintaining, and managing Cisco security solutions

- Informal technical updates on a topic that is mutually agreed upon and relevant to security technologies, and,
  - Chalk talks,
  - Shadowing and mentoring as needed to assist your staff in assuming responsibility for Cisco security solution,
- Ongoing consultation to answer questions as needed for 30 days after a deployment.

Specific Service Responsibilities of the Customer

Customer is responsible for the following:

- Provide details on desired/requested topics Customer wants to see covered during the knowledge transfer and mentoring sessions.
- Provide background information on the Customer participant skill sets for the knowledge transfer or mentoring sessions.
- Provide Customer facilities and equipment (such as conference rooms, white boards, projectors) and make them available to host the informal technical update sessions.

Security Strategy and Planning Support

Specific Service Responsibilities of Cisco

Cisco will provide strategic and tactical guidance via a series of meetings or workshop around a Customer selected security topic followed by a workshop for up to three (3) days to work through the incubation and strategy process covering topics that may include but are not limited to security technologies, cloud, TrustSec and identity, IT GRC (Governance, Risk Management and Compliance), TeleWorking, management, data center and collaboration security. Cisco responsibilities include:

- Briefing Customer on the service and service options.
- Conduct a Customer pre-planning workshop.
- Conducting Customer planning workshop.
- Capture synopsis and recommendations from workshop.
- Post-workshop analysis.
- Conduct post-workshop follow-up meeting.
- Capture synopsis and final recommendations post-workshop meeting.
- Create Work Summary and submit for Customer Review

Limitations:

Each unit of Security Strategy and Planning Support includes:

- Up to three (3) major challenge areas.
- Up to three (3) meetings or one (1) full-day pre-workshop meeting.
- Up to three (3) days for an onsite, offsite, or TelePresence workshop.
- Up to three (3) follow-up meetings or one (1) full-day post-workshop meeting.
- Up to four (4) concurrent Cisco participants.

Specific Service Responsibilities of the Customer

Customer responsibilities include:

- Ensure all key stakeholders participate in Cisco briefing on the service and service options.
- Ensure all key stakeholders participate in the Cisco conducted meetings and workshops.
- Prepare for workshop and provide detailed briefing with supporting facts.
- Review and approve the Work Summary Review.

Security Technology Readiness Assessment

Specific Service Responsibilities of Cisco

Cisco will work with Customer to define the Customer's business, technical and operational requirements, analyzing implementation requirements for a new security solution and assess the readiness of Customer's Network devices, operations, security policies, and architecture to support the solution Cisco is responsible for the following:

- Deliver the STRA questionnaire at least seven (7) business days prior to design workshop.
- Conduct design workshop to review STRA questionnaire.

- Analyze implementation requirements for a new security technology and assess the readiness of Customer's infrastructure, operations, security policies, and architecture to support the solution.
- Develop Security Readiness Assessment Report to document findings and recommendations including recommendations for modifications to the network infrastructure and to configuration parameters for application performance and availability.
- Conduct an interactive meeting with the customer to review all findings and develop steps to address gaps to ensure that the environment is ready to support the new technology.

Limitations:

Each unit of Security Technology Readiness Assessment includes:

- Up to one (1) security technology (i.e. Cisco ISE, AnyConnect Remote VPN, 802.1x deployments)
- Up to two (2) network segments with a total of up to ten (10) customer device classes. A class is defined as a group of devices (i.e. firewalls or routers) with similar configurations.

Specific Service Responsibilities of the Customer

Customer is responsible for the following:

- Respond to STRA questionnaire at least two (2) business days prior to design workshop.
- Ensure that appropriate customer engineers and management participate in the design workshop.
- Actively participate in development of steps to address changes required to ensure the network is ready to support the new technology.

Security Validation and Testing Premier Support

Specific Service Responsibilities of Cisco

Cisco will consult with Customer via a series of meetings to develop a thorough understanding of Customer's solution-oriented testing goals and requirements Cisco will execute networking tests and report findings to Customer. Support may include, among other information, the following:

- Provide Customer with Request for Validation and Testing Support Questionnaire, and a sample report.
- Review the Request for Validation and Testing Support Questionnaire.
- Meet with Customer to discuss responses to the Request for Validation and Testing Support Questionnaire, which may include the goals, business and technical requirements, testing methodology, Cisco standard validation and testing deliverable document format.
- Create and review the Test Plan with Customer.
- Provide Customer with requirements including lab facility, equipment, software, cabling, and interface requirements.
- Execute Test Plan upon Customer acceptance of Test Plan and Testing Schedule.
- Perform and document Test Results Analysis.
- Review Validation and Testing Report with customer.
- Review Customer feedback.
- Finalize and submit Validation and Testing Report to Customer.
- Provide local support at the Cisco lab facility, as needed, during remote testing. For example: in the event of a cable or connector failing during testing, then Cisco is responsible for providing replacement cable or connector.
- Provide Lab facility, equipment, software, cables, connectors, etc. required to perform testing.
  Set-up Lab, including rack and stack of equipment, cabling of power and network connections, confirmation of power-on self-test of equipment, confirmation of software version, and initial device configurations.

Cisco will utilize the following services and lab equipment to deliver Security VTPS

- 320 to 400 hours of Expertise, Test Engineer
- 80 Hours of Program management
- Up to $1.5M GPL List of HW (Included)

Limitations:

Each unit of Security Validation and Testing Support includes:

- Up to two (2) weeks for methodology development
- Up to two (2) weeks for test plan development.
- Up to one (1) week for Cisco site test lab setup
- Up to two (2) weeks design validation testing.
- Up to one (1) week results analysis.

Most engagements are between eight (8) and ten (10) weeks.

Specific Service Responsibilities of the Customer

Customer is responsible for the following:

- Complete the Request for Validation and Testing Support Questionnaire, which may include information such as goals, business and technical requirements, desired features and functionality, network diagrams, desired test plan and success criteria, and desired testing methodology.
- Provide appropriate production device configurations, if needed, for testing.
- Provide a designated single point of contact with authority to approve decisions.
- Provide Customer support as needed for third-party or Cisco competitor products.
- Provide equipment (including shipping to Cisco lab) some third-party or Cisco competitor products.

Security Validation and Testing Support

Specific Service Responsibilities of Cisco

Cisco will consult with Customer via a series of meetings to develop a thorough understanding of Customer's solution-oriented testing goals and requirements Cisco will execute networking tests and report findings to Customer. Support may include, among other information, the following:

- Provide Customer with Request for Validation and Testing Support Questionnaire, and a sample report.
- Review the Customer completed Request for Validation and Testing Support Questionnaire.
- Meet with Customer to discuss responses to the Request for Validation and Testing Support Questionnaire, which may include the goals, business and technical requirements, testing methodology, Cisco standard validation and testing deliverable document format.
- Create and review the Test Plan with Customer.
- Provide Customer with requirements including lab facility, equipment, software, cabling, and interface requirements.
- Execute Test Plan upon Customer acceptance of Test Plan and Testing Schedule.
- Perform and document Test Results Analysis.
- Review Validation and Testing Report with customer.
- Review Customer feedback.
- Finalize and submit Validation and Testing Report to Customer.

Limitations: On Customer Site / Location

- Equipment supplied by Customer.
- Up to one (1) week for testing setup.
- Up to two (2) weeks of lab execution.
- 200 hours of Expertise, Test Engineer.
- 40 Hours of Program management.
- T&E as needed.

Other limitations include:

- Security Validation and Testing Support is not offered in every geography or location.

Specific Service Responsibilities of the Customer

Customer is responsible for the following:

- Complete the Request for Validation and Testing Support Questionnaire, which may include information such as goals, business and technical requirements, desired features and functionality, network diagrams, desired test plan and success criteria, and desired testing methodology.
- Provide Lab facility, equipment, software, cables, connectors, etc. required to perform testing.
- Provide appropriate production device configurations, if needed, for testing.
- Set-up Lab, including rack and stack of equipment, cabling of power and network connections, confirmation of power-on self-test of equipment, confirmation of software version, and initial device configurations (in cases such as production deployment re-creations).
- Provide local support, as needed, during onsite and remote testing. For example: in the event of a cable or connector failing during testing, then customer is responsible for providing replacement cable or connector.
- Provide Customer support as needed for some third-party or Cisco competitor products.

Software Security Alert

Cisco will provide proactive analysis of the security advisories (PSIRTs) that Cisco generates when security issues are uncovered that may impact networks in which Cisco products operate and the necessary action to repair and/or protect the network from these issues. After Cisco publicly releases the security advisory, the assessment is delivered to the Customer via the Software Security Alert (SSA). Cisco will provide an analysis of the vulnerability and its resolution with regard to its possible impact on the Customer's Security solution.

- Analysis of how a Cisco Security Advisory may or may not affect Customer's Network,
- Recommendations to mitigate risk, and,
- List of affected or potentially affected Networking devices.

Specific Service Responsibilities of the Customer

Customer is responsible for the following:

- Provide Cisco with a designated contact to handle all Security related announcements.

Specific Advisory Service Details (CON-AS-SECADV)

This section provides the service details for the following Advisory services:

- Incident Response Retainer
- Security Ongoing Flexible Support
- Security Consulting Services
  - Security Program Assessment and Strategic Roadmap
  - Commercial Security Program and Control Design Assessment
  - Application Architecture Assessment
  - Application Penetration Assessment
  - SDLC Improvement
  - Mobile Application Assessment
  - Network Architecture Assessment
  - Network Penetration Test
  - Wireless Security Assessment
  - Physical Security Assessment
  - Social Engineering
  - Red Team
  - Mobile Security Strategy Workshop
  - Cloud Security Strategy Workshop
  - Cloud Compliance Health Check
  - Cloud Architecture Assessment
  - Security Metrics Workshop
  - Third Party Assessment
  - Privacy Impact Analysis
  - Security/IT Risk Program Support Staff Augmentation
  - Information Security Program Development
  - Information Security Risk Program Development
  - Information Security Risk Assessment
  - Security Metrics Program Development
  - Third Party Risk Program Development
  - Assessment of Organizational Alignment to ISO 27001
  - Assessment of Organizational Alignment to ISO 27002
  - HIPAA and HITECH Assessment
  - PCI ASV Scanning Service
  - PCI-DSS Readiness Assessment
  - Enterprise Security Advisor
  - Security Segmentation Service

Further, as a condition to Cisco providing the following Advisory Services, Customer understands, acknowledges and agrees as follows:

- Customer has given permission to Cisco to conduct testing on the system under test in line with the terms this Service Description. Cisco will conduct such tests as they deem necessary during mutually agreed periods of time. These tests may include activities that might otherwise be construed as unethical and unlawful. The Customer hereby authorizes such tests to be conducted. It is at the discretion of the Customer as to whether or not they inform their Internet Service Provider (ISP) or any other service provider affected by the testing, that testing is taking place. The Customer, therefore, accepts the responsibility should such a service provider act in any way that affects the outcome of the test or even causes the testing to be suspended. Cisco shall take every precaution to avoid damage to the system under test including any data stored upon it, however, it is understood by the Customer that such damage may occur, and that the risk, minimal though it may be, is accepted by the Customer.

Incident Response Retainer

Cisco Incident Response Retainer service provides review & evaluation of Customer's incident readiness program.

Specific Service Responsibilities of Cisco

Cisco may provide any or all of the following Incident Response (IR) deliverables as part of the retainer: incident readiness activities, incident response strategy and planning, tabletop exercises, proactive threat hunting, and emergency incident response which can include triage, coordination, investigation (e.g. analysis and forensics), containment, and remediation. Cisco responsibilities include:

- Working with Customer to define how to leverage subscription hours.
- Provide emergency access to Incident Response services for the duration of the subscription.
- Provide an Incident Response resource within four (4) hours remotely via telephone.
- As requested, begin deployment of personnel to Customer location within 24 hours.
- Monthly status update specific to the Customer's environment.

Limitations:
Given the variety of situations and issues that may be encountered, incidents may require a variety of services to compliment this service. For example, incidents may require specialized tools to provide deeper visibility or access into the network.

Other limitations include:

- There is no guarantee that root-cause analysis will result in a root-cause being identified or confirmed for an incident
- Reasonable efforts will be made to provide conclusive findings and an issue resolution plan.
- IR services can provide insight into deficiencies of an IR strategy and a plan for resolving; however, executing the plan may require follow-on services.
- Work may occur after Standard Business Hours.
- Any hours not used during the term of the subscription retainer will be forfeited.

Each unit of Security IR Service includes:

- 160 hours, including two (2) trips with eight (8) hours of travel each

Specific Service Responsibilities of the Customer

Customer responsibilities include:

- Designate person(s) from within its organization to serve as a liaison to Cisco.
- Provide reasonable electronic access to Customer's Network and security devices to enable Cisco in providing support.
- Ensure access to Incident Response strategy information, to include processes and workflows, is made available to Cisco.

Security Ongoing Flexible Support

Cisco will provide informal, Ongoing Flexible Support for incremental changes to the network security architecture. This flexible support may be applied to other work items within Security Optimization Service and 1 Unit is limited to 40 hours of assigned engineer's time. Cisco engineers will be assigned as work items are selected throughout the term of the service contract.

Specific Service Responsibilities of the Customer

Customer responsibilities include:

- Provide Cisco with details around what type of support is needed when a request is made.

Security Consulting Services

Cisco Security Advisory Team delivers a broad range of security, risk, and compliance advisory services required to support secure operations of an enterprise or government agency.

Assessment & Penetration Services include:

- Application Penetration Assessment
- Mobile Application Assessment

- Network Penetration Test
- Wireless Security Assessment
- Physical Security Assessment
- Social Engineering
- Red Team
- Information Security Risk Assessment
- Third-party Risk Assessment

Program & Architecture Services include:

- Assessment of Organizational Alignment to ISO 27001/27002
- Security Program Assessment & Strategic Roadmap
- Commercial Security Program & Control Design Assessment
- Security Metrics Workshop
- Application Architecture Assessment
- Cloud Architecture Assessment
- Network Architecture Assessment
- Mobile Security Strategy Workshop
- Cloud Security Strategy Workshop
- SDLC Improvement
- Third-party Risk Program Development
- Privacy Impact Analysis
- Security Risk Program Support Staff Augmentation
- Security Segmentation Services
- Enterprise Security Advisor
- Information Security Program Development
- Information Security Risk Program Development
- Security Metrics Program Development

Compliance Services include:

- HIPAA & HITECH Assessment
- PCI ASV Scanning Service
- PCI-DSS Readiness Assessment
- Cloud Compliance Health Check

The details of these services are as below.

Security Program Assessment and Strategic Roadmap

Specific Service Responsibilities of Cisco

Cisco will work with the Customer to perform the following as part of Security Program Assessment & Strategic Roadmap

- Conduct workshop/interactive meetings with Customer to review the documents and perform controlled inspection across the enterprise.
- Work with the Customer to determine current state capabilities, identify future state capabilities based on business requirements.
- Develop a detailed roadmap of initiatives over time to achieve target state.
- Develop Security Program Assessment report to document findings and recommendations.
- Provide a Strategic Roadmap of initiatives for Customer enterprise environment.
- Provide an executive summary presentation.

Specific Service Responsibilities of Customer

- Provide access to the appropriate resources with knowledge and authority to work with Cisco during the assessment workshop.
- Designate person(s) from within its organization to serve as a liaison to Cisco
- Provide reasonable electronic access to Network and security devices to enable Cisco during the workshop meetings.

Commercial Security Program and Control Design Assessment

Specific Service Responsibilities of Cisco

- Perform assessment and reviews of design of an organization's security program and supporting controls across critical areas of analysis
- Provide current design effectiveness as well as required end state.
- Provide recommended roadmap to address Customer's desired end state.
- Develop Security Program and Control Design Assessment report to document findings and recommendations.
- Provide an executive summary presentation.

Specific Service Responsibilities of Customer

- Provide access to the appropriate resources with knowledge and authority to work with Cisco during the assessment workshop.
- Designate person(s) from within its organization to serve as a liaison to Cisco
- Provide reasonable electronic access to Network and security devices to enable Cisco during the workshop meetings.

Application Architecture Assessment

Cisco will review application documentation and conduct interviews with application subject matter experts to identify new ways to strengthen the application and its infrastructure. A single application will be evaluated by performing up to forty (40) interviews and eighty (80) documentation reviews.

Specific Service Responsibilities of Cisco

- Review the application requirements with Customer's designated business and technical representatives to identify the business drivers, service capabilities, and specific areas of concern related to security.
- Review the Customer's existing architecture with Customer's designated technical and business representatives to gain an understanding of systems, controls, and requirements.
- Analyze the existing application design with respect to security requirements and practices.
- Evaluate specific areas of the design through technical interviews, documentation reviews, data flow analysis, threat modeling, and workshops conducted with both business and technical stakeholders.
- Identify where sensitive data is stored and how it is accessed.
- Identify areas of potential weakness in the application's external interfaces, internal component communication, data storage, and transaction processing.
- Identify security vulnerabilities and the impact associated with the most-likely and worst-case exploitation scenarios.
- Analyze existing application security architecture components, including:
    - Administration
    - Auditing and Monitoring
    - Authentication and Authorization
    - Configuration Management
    - Information Integrity and Confidentiality (Cryptography, Data Validation, Data-at-Rest Protection, Data-in-Transit Protection)
    - Logging and Error Handling
    - Session Management
    - Third Party Dependencies
- Determine the best approach to assess individual application components, with minimal disruption to the production environment, including:
    - Penetration Testing
    - Source Code Analysis
    - System or Application Configuration Review
- Document recommendations for improving the application's security in the Application Architecture Assessment Report which includes:
    - Executive summary

  - Scope and methodology
  - Analysis of application's security architecture
  - Logical architectural diagrams that display data flows and components
  - Prioritized recommendations
  - Recommendations for next steps
- Provide the Application Architecture Assessment Report to Customer for review and approval.

Specific Service Responsibilities of Customer

- Ensure appropriate application business owners, architects, developers, security, third parties, and IT operations personnel participate with Cisco in the Services, as required.
- Provide Cisco with existing documentation, including architecture and design documents and policies and procedures.
- Review and approve the Application Architecture Assessment Report.

Application Penetration Assessment

Cisco will perform an Application Penetration Assessment of a single application for a single platform. The assessment will begin by identifying the application's immediate attack surface. The attack surface will be analyzed for vulnerabilities using manual and automated testing techniques. Source code may be leveraged to increase testing efficiency. When access credentials are provided, Cisco will perform authenticated testing. The primary focus of the testing is to identify application-layer vulnerabilities in Customer developed code; however, the testing may discover vulnerabilities in the application's immediate dependencies. The application shall not exceed 250,000 lines of code. The assessment will evaluate up to sixty (60) application inputs (e.g., RPC calls, HTTP POST requests, or web service messages processed by the application) with an average of fifteen (15) parameters per input, across a maximum of six (6) user roles.

Specific Service Responsibilities of Cisco

- Perform an assessment to identify security relevant issues including the following classes of vulnerabilities:
  - Injection vulnerabilities (command injection, SQL injection)
  - Cross-site scripting (XSS) and other script-based injection vulnerabilities
  - Cross-site request forgery (CSRF)
  - Memory management vulnerabilities
  - Input and output validation vulnerabilities
  - Session management vulnerabilities
  - Access control vulnerabilities
  - Path canonicalization vulnerabilities
  - Insufficient or ineffective use of encryption
  - Application related denial of service
  - Sensitive information exposure
  - Secure secrets storage
  - General data handling vulnerabilities
  - Object reference vulnerabilities
  - Design or logic that may introduce security weaknesses
  - Configuration weaknesses
  - Communication security weaknesses
  - Applicable issues not explicitly identified above, but covered by pertinent standards (OWASP Top 10, SANS Top 25)
- Conduct an analysis which includes a range of techniques intended to identify security vulnerabilities in the most expedient manner possible. Cisco will apply the following core strategies in performing the assessment:
  - Attack surface enumeration: attempts to identify application functionality by automated traversal of site hierarchy and permuting common variations on popular naming conventions
  - Automated fault injection: automated submission of a range of malicious data to identify security vulnerabilities in the request path
  - Manual fault injection: manual submission of malicious data to identify security vulnerabilities in the request path; d) Known vulnerability testing: identification of vulnerabilities in the hosting platform (web server, servlet container) using primarily automated analysis techniques
  - Code comprehension: manual source code analysis of security-relevant code paths, when code is available
  - Candidate point: automated analysis to pinpoint known vulnerability patterns, followed by manual analysis to validate any vulnerability candidates, when code is available
  - Data correlation (Research vulnerabilities, eliminate false positives, Investigate the extent of the findings)
- Create the Combined Application Assessment Report which includes:
  - Executive summary
  - Scope and approach
  - Detailed list of findings
  - Details of vulnerabilities discovered (risk, severity rating, likelihood of attack or skills required)
  - Remediation recommendations

    - Analysis of security impact
- Provide the Application Penetration Assessment Report to Customer for review and approval.

Specific Service Responsibilities of Customer

- Ensure key individuals participate with Cisco for interviews and addressing technical issues and questions.
- Provide Cisco with existing application diagrams and documentation, if available.
- Identify two (2) user accounts for each role to be tested during the assessment.
- Provide Cisco with all information needed to access the application (e.g., domain names, URLs, IP addresses).
- Provide Cisco with all information needed to fully exercise the application (e.g., example code, API documentation)
- Agree with Cisco on available hours and days for testing.
- Provide Cisco with administrative-level access to systems under assessment or access to Customer personnel capable of performing administrative actions in the event of technical difficulties.
- Provide Cisco with application source code for application(s) being assessed, if applicable.
- Identify any specifically targeted modules and their size, if applicable.

- Provide debug and production builds of target software, when applicable.
- Provide access to testing and production environments, when applicable.
- Cover all costs associated with increased resource utilization on third-party systems (e.g., Cloud providers) required by the testing.
- Notify and obtain testing authorization from any interested third-parties.
- Allow Cisco equipment and tools to be placed on and used against the target environment.
- Review and approve the Application Assessment Report.

SDLC Improvement

Cisco will review the Software Development Life Cycle ("SDLC") to identify security deficiencies in the development process. A Secure SDLC Review includes interviews, a review of current security policies and standards, and an analysis of current practices. Based on the findings, Cisco will provide guidance for developing more secure software development and quality assurance policies, processes, and standards.

Specific Service Responsibilities of Cisco

- Review existing collateral that is relevant to the current software development lifecycle process, including:
    - Secure coding standards
    - Data classification policies
    - Testing procedures
    - Training standards
    - Regulatory and contractual compliance requirements
    - Documentation of security standards enforced within the organization
    - Any existing metrics used to measure security practices within the organization
    - Any other relevant supporting documentation
- Interview key Customer personnel, including:
    - Management staff familiar with the governance of existing security practices
    - Development staff
    - Testing staff
    - IT staff
    - Support staff
- Create the SDLC Assessment Report which includes:
    - Executive summary
    - Scope, description of work performed, and methodology
    - Identification of gaps and recommended remediation related to governance, operational practices, and technical controls
    - Recommendations for next steps
- Provide the SDLC Assessment Report to Customer for review and approval.

Specific Service Responsibilities of Customer

- Ensure key individuals participate with Cisco in interviews and addressing technical questions.
- Provide Cisco with existing software development diagrams and documentation, including:
    - Development policies and procedures
    - Security awareness and training documentation
    - Corporate security policy
    - Testing procedures and standards
    - Example application specific documents (UML documents, data flows, schema)

  - Data classification standards
  - Access to application code repository
- Review and approve the SDLC Assessment Report.

Mobile Application Assessment

Cisco will perform a Mobile Application Assessment of a single mobile application for a single platform. The Mobile Application Assessment will begin by identifying the application's immediate attack surface. The attack surface will be analyzed for vulnerabilities using manual and automated testing techniques. When access credentials are provided, Cisco will perform authenticated testing. The primary focus of the testing is to identify application-layer vulnerabilities in Customer developed code; however, the testing may discover vulnerabilities in the application's immediate dependencies. The application shall not exceed 250,000 lines of code. The assessment will evaluate up to sixty (60) application inputs (e.g., RPC calls, HTTP POST requests, or web service messages processed by the application) with an average of fifteen (15) parameters per input, across a maximum of three (3) user roles.

Specific Service Responsibilities of Cisco

- Perform an assessment to identify security relevant issues including the following classes of vulnerabilities:
  - Injection vulnerabilities
  - Cross-site scripting (XSS) and other script-based injection vulnerabilities
  - Cross-site request forgery (CSRF)
  - Memory management vulnerabilities
  - Input and output validation vulnerabilities
  - Session management vulnerabilities
  - Access control vulnerabilities
  - Path canonicalization vulnerabilities
  - Insufficient or ineffective use of encryption
  - Application related denial of service
  - Sensitive information exposure
  - Use of insecure local storage
  - Insufficient use of transport layer protection for mobile data traffic
  - Insecure use of inter-process communication interfaces
  - General data handling vulnerabilities
  - Design and logic vulnerabilities
  - Unnecessary services
  - Mobile-specific service interfaces (e.g. SMS)
  - Applicable radio communication (e.g. Bluetooth)
  - Applicable issues not explicitly identified above, but covered by pertinent standards (OWASP Top 10, SANS Top 25)
- Conduct an analysis which includes a range of techniques intended to identify security vulnerabilities. Cisco will apply the following core strategies in performing the assessment:
  - Attack surface enumeration: attempts to identify application functionality by automated traversal of site hierarchy and permuting common variations on popular naming conventions
  - Manual fault injection: manual submission of malicious data to identify security vulnerabilities in request path
  - Automated fault injection (fuzzing): automated submission of a range of malicious data to identify security vulnerabilities in request path
  - Known vulnerability testing: identification of vulnerabilities in the hosting platform (web server, servlet container) using primarily automated analysis techniques
  - Code comprehension: manual source code analysis of security-relevant code paths
  - Candidate point: automated analysis to pinpoint known vulnerability patterns, followed by manual analysis to validate any vulnerability candidates
  - Data correlation (Research vulnerabilities, eliminate false positives, Investigate the extent of the findings)
- Create the Mobile Application Assessment Report which includes:
  - Executive summary
  - Scope and approach
  - Detailed list of findings
  - Details of vulnerabilities discovered (risk, severity rating, likelihood of attacks or skills required)
  - Remediation recommendations
  - Analysis of security impact
- Provide the Mobile Application Assessment Report to Customer for review and approval.

Specific Service Responsibilities of Customer

- Ensure key individuals participate with Cisco in interviews and addressing technical questions.
- Provide Cisco with existing application diagrams and documentation, if available.

- Identify two (2) user accounts for each role to be tested during the assessment.
- Provide Cisco with all information needed to access the application and supporting components (e.g., web services, domain names, URLs, IP addresses).
- Provide Cisco with all information needed to fully exercise the application (e.g., example code, API documentation). Provide mobile application simulator and project files to duplicate development execution environment
- Provide Cisco with mobile device and data cables for connecting to PC/Mac, if required.
- Assist with emulated environment specifications and testing setup through direct access (telephone or e-mail) to Customer development team member.
- Agree with Cisco on available window of hours for testing.
- Provide Cisco with administrative-level access to systems under assessment or access to Customer personnel capable of performing administrative actions in the event of technical difficulties (such as account lockout or system failure).
- Provide Cisco with application source code for application(s) being assessed, when available.
- Identify any specifically targeted modules and their size in source lines of code, if applicable.
- Provide debug and production builds of target software, when applicable.
- Provide access to testing and production environments.
- Notify and obtain testing authorization from any interested third parties.
- Allow Cisco equipment and tools to be placed on and used against the target environment.

- Review and approve the Mobile Application Assessment Report.

Network Architecture Assessment

Cisco will conduct a Network Architecture Assessment to identify the security architecture of the target network. The Network Architecture Assessment will assess the network within the context of Customer's business and technical requirements. Cisco will propose solutions to eliminate security weaknesses in network's design and implementation. A single network will be evaluated by performing up to twenty (20) interviews, forty (40) documentation reviews, and twenty (20) configuration file reviews.

Specific Service Responsibilities of Cisco

- Review the network technical requirements including technical specifications, high-level design documents, and technologies in use.
- Review the network business requirements with designated business and technical representatives to identify the business drivers, service capabilities, and specific areas of security-related concern.
- Review architecture with designated technical and business representatives to gain an understanding of systems, controls, and requirements.
- Analyze the network design with respect to security requirements and practices.
- Review relevant documentation, including technical design documents, process flows, and security architecture to identify potential vulnerabilities.
- Perform interviews with subject matter experts
- Perform analysis of a small set of representative configuration files
- Perform a gap analysis of key secure network components, such as:
    - Identity and Access Management (IAM)
    - Key Management System (KMS)
    - Multi-Factor Authentication (MFA)
    - Secure Remote Access (e.g., VPN)
    - Network Access Control (NAC)
    - Wireless Security Configuration and Appliances (e.g., WIPS)
    - Network Intrusion and Prevention Systems (NIDS/NIPS)
    - Mobile Device Management (MDM)
    - Data Leakage Prevention (DLP)
    - Application Layer Gateways (ALG; e.g., web and e-mail gateways)
    - End-point Protection
    - Security and Information Event Management (SIEM)
    - File Integrity Monitoring (FIM)
    - Availability Monitoring
    - Load Balancing, High-Availability (HA), and Virtualization
    - DDoS Protection
    - DNS and NTP architecture
    - Network Segmentation
    - System Backup
    - Incident Response
    - System Inventory

  - System Provisioning
  - Patch Management
  - Configuration Management
  - Change Management
  - Vulnerability Management
- Create the Network Architecture Assessment Document which includes:
  - Executive summary
  - Management summary, including objectives and process information
  - Assessment of the security measures currently in place compared with industry good practice
  - Analysis of the network security architecture
  - Analysis of security issues identified, estimated business impact (if possible), and recommendation for remediation
  - Prioritized list of recommendations
- Provide the Network Architecture Assessment Document to Customer for review and approval

Specific Service Responsibilities of Customer

- Provide Cisco with access to the business site during Standard Business Hours including buildings, parking, phone systems, internet access, server rooms, and workstations.
- Provide Cisco with access to a suitable conference room facility for meetings, interviews, and facilitated sessions during on-site components of the engagement.

- Provide Cisco with accurate and detailed business requirements documentation for the networks, such as business drivers, service requirements, identification of critical processing and data concerns, and deployment procedures.
- Provide Cisco with accurate and detailed technical requirements documentation for the networks, including technical specifications, high-level design diagrams, technologies used, developer documentation, design documentation, and use-case diagrams.
- Provide Cisco with access to network architects, engineers, administrators, and other subject matter experts to conduct interviews and workshops
- Provide Cisco with configuration files, system inventory, policy and procedures
- Review and approve the Network Architecture Assessment Document.

Network Penetration Test

Cisco will perform an external or internal Network Penetration Test of a single Customer network. The primary objective of the test is to gain access to valuable systems and data. The testing will attempt to identify high risk, exploitable vulnerabilities and provide an opportunity to measure the effectiveness of security investments against a simulated threat. Up to 256 external IP addresses or 400 internal IP addresses will be tested.

Specific Service Responsibilities of Cisco

- Perform intelligence gathering as follows:
  - Perform perimeter scans of protocols, services, operating systems, and other technologies
  - Identify security defenses to be circumvented
  - Identify system trust and users
  - Identity system components
  - Construct a view of the attack surface
- Perform threat modeling, vulnerability discovery, and attack surface analysis as follows:
  - Perform automated and manual scanning
  - Perform limited fuzzing and reverse engineering, if required
  - Research applicable threats to system assets and software
  - Prioritize attacks based on testing objectives
- Perform the following exploitation activities, where applicable:
  - Exploit design and architectural weaknesses by performing network sniffing and man-in-the-middle attacks
  - Compromise system components by exploiting implementation weaknesses in software through buffer overflows, remote code execution, cross-site scripting, SQL injection, and other command injection attacks
  - Test operational weaknesses within patch management, configuration management, and system deployment practices
  - Exploit user weaknesses through password guessing and password cracking attacks
  - Circumvent security controls by evading firewalls, intrusion detection systems, anti-virus, access controls, cryptographic protections, and data loss prevention systems
- Perform the following post-exploitation activities, where applicable:
  - Leverage discovered vulnerabilities to establish persistence
  - Leverage discovered vulnerabilities to escalate privileges
  - Search for credentials and sensitive data (e.g., personally identifiable information, credit card numbers)

  - Attempt to pivot attacks to additional targets
  - Attempt to exfiltrate data, as approved by the Customer
- Provide the following reporting:
  - Eliminate false positives, where possible
  - Investigate potential business impact
  - Investigate and develop remediation strategies
- Create the Network Penetration Test Document which includes:
  - Executive summary
  - Scope and approach
  - Prioritized list of findings
  - Details of security issues discovered including: risk, severity rating, likelihood of attack or skills required, remediation recommendations, analysis of security impact
- Provide the Network Penetration Test Document to Customer for review and approval.

Specific Service Responsibilities of Customer

- Provide Cisco with accurate and detailed technical requirements documentation for the networks, including technical specifications, high-level design diagrams, technologies used, developer documentation, design documentation, and use-case diagrams.
- Provide Cisco with access to key individuals for technical questions.
- Provide Cisco with available window of hours for testing.

- Provide Cisco with target identification information (e.g., IP addresses, hostnames, URLs).
- Allow Cisco equipment and tools to be placed on and used against the target environment.
- Review and approve the Network Penetration Test Document.

Wireless Security Assessment

Cisco will conduct a Wireless Security Assessment of a single location. Cisco will enumerate up to 5 unique, SSID-identified, wireless networks and evaluate the deployment of the wireless environment for vulnerabilities. Security weaknesses may be demonstrated by exploiting the discovered weaknesses after Customer approval is provided.

Specific Service Responsibilities of Cisco

- Perform reconnaissance to enumerate both corporate 802.11 a/b/g/n/ac wireless access points.
- For access points that are identified and to the extent possible, Cisco will attempt to gather the following information:
  - SSID
  - Configuration state of SSID broadcasting
  - Type of authentication and encryption
- Assess the risk of wireless devices by attempting to identify the following:
  - Customers that bridge wireless networks to the corporate network, if credentials are provided
  - Wireless clients that commonly join insecure wireless networks
  - Weak authentication configuration (e.g., disabled certificate validation)
- Assess the overall wireless deployment, including:
  - Administration
  - Network connectivity and segmentation
  - Access point configuration
  - Authentication and encryption
- Identify and validate vulnerabilities.
- Rank vulnerabilities based on associated risk.
- Create the Wireless Security Assessment Report which includes:
  - Executive summary
  - Scope and approach
  - Prioritized list of findings
  - Details of security issues discovered, including: risk, severity rating, likelihood of attack or skills required, remediation recommendations, analysis of security impact
- Provide the Wireless Security Assessment Report to Customer for review and approval.

Specific Service Responsibilities of Customer

- Provide Cisco with access to the business site during Standard Business Hours including buildings, parking, telephone systems, internet access, server rooms, and workstations.
- Provide Cisco with access to a suitable conference room facility for meetings, interviews, and facilitated sessions during on-site components of the engagement.
- Provide Cisco with accurate and detailed technical requirements documentation for the wireless networks, including technical specifications, high-level design diagrams, technologies used, design documentation, and use-case diagrams.

- Provide Cisco with access to key individuals for technical questions.
- Provide Cisco with available window of hours for testing.
- Provide Cisco with unique identification of target wireless devices.
- Provide Cisco with authorization to exploit identified vulnerabilities, when required.
- Allow Cisco equipment and tools to be placed on and used against the target environment.
- Review and approve the Wireless Assessment Report.

Physical Security Assessment

Cisco will perform a Physical Security Assessment of a single low-security facility. A low-security facility does not contain mantraps, biometrics, or armed guards. The primary objective of the test is to gain access to valuable material and secure areas. The testing will attempt to exploit weaknesses in physical security controls to provide an opportunity to measure the effectiveness of physical security defenses and improve security awareness training efforts.

The Physical Security Assessment will be conducted on-site.

Specific Service Responsibilities of Cisco

- *Intelligence Gathering and Planning*
  - Use Open Source Intelligence (OSINT) techniques to gain intelligence about the physical target and relevant personnel.
  - Perform a site survey of the location's access control mechanism and procedures.
  - Identify security defenses for circumvention.

  - Identify system trust and personnel.
  - Develop a plan to achieve mission objectives.
  - Compose a tailored physical attack kit to be used during the exploitation and post-exploitation phases.

- *Exploitation*
  - Attempt to penetrate the perimeter of each physical location using multiple techniques such as:
    - Develop a fake identify and provisional purpose for being on-site.
    - Attempt to gain physical access to defined facilities or areas (e.g., tail-gating).
    - Compose fake badges or business cards, when needed.
    - Attempt to gain physical access by attacking physical control systems (e.g., lock-picking, RFID cloning)
    - Develop attack infrastructure to monitor for connections from infected devices.
    - Place infected USB devices, CDs, and small computing devices in high-traffic user areas.
    - Monitor for connections from USBs, CDs, and computing devices within the testing timeline.
    - Impersonate Customer employees, vendors, or customers.
    - Attempt to convince personnel to perform actions on behalf of the tester (e.g., opening doors and locks).
    - Attempt to obtain access to Customer defined devices or material.
    - Attempt to circumvent and exploit weaknesses in physical security controls.
    - Attempt to evade physical monitoring detection systems such as cameras and door alarms.

- *Post-Exploitation*
  - Attempt to gain access to additional restricted locations.
  - Attempt to gain access to sensitive material.
  - Plant rogue devices like implants, key loggers, and USB devices when relevant.
  - Attempt to exfiltrate equipment or material, as approved by the Customer.
  - Document access and access path to defined objectives.
  - Provide the Physical Security Assessment Report to Customer for review and approval.

Specific Service Responsibilities of Customer

- Provide addresses for the physical location to be tested.
- Provide clear directions on reaching and identifying the physical location.
- Identify secure areas.
- Provide support to gain access to any physical locations required to begin testing the physical locations in scope for testing.
- Provide details regarding any hazards at each physical location (e.g., armed guards, health hazards).
- Provide a written testing authorization letter that can be provided to security personnel.
- Identify consultants by name in the authorization letter.
- Identify any equipment or material that is authorized to be taken off the premises in the authorization letter.
- Provide timely response if local authorities detain Cisco personnel.
- Notify and coordinate the testing activities with any interested parties (e.g., building management and security guards).
- Obtain testing authorization from property owners if the physical location is shared or leased.
- Review and approve the Physical Security Assessment Report.

Social Engineering

Cisco will perform text- or voice-based Social Engineering for the Customer. For text-based social engineering, up to five-hundred (500) Customer-supplied e-mail addresses or thirty (30) Cisco-discovered but Customer authorized e-mail addresses will be subject to phishing attacks. For voice-based social engineering, attempts to contact up to fifteen (15) employees will be made. The primary objective of the exercise is to identify individuals requiring additional security awareness training or obtain generalized security awareness training success metrics that do not identify individuals (i.e., anonymized results). The testing may use communication mechanisms such as e-mail, instant messaging, phone, and fax to convince individuals to compromise security in a controlled environment.

The Social Engineering Assessment will be conducted from one or more remote locations.

Specific Service Responsibilities of Cisco

- *Text Based Social Engineering*
  - Provide Customer with the source IP address(es) of the e-mail server(s) used to execute the campaign.
  - Identify highly exposed users using Open Source Intelligence (OSINT) methods.
  - Develop up to four (4) phishing campaigns designed to convince targeted users to:
    - Disclose access credentials
    - Perform actions on behalf of the tester
    - Visit attacker controlled websites
    - Open attacker provided files
  - Develop and customize attack infrastructure, which may consist of:
    - Building custom web-sites
    - Constructing or deploying custom pseudo-malware and backend command and control servers
  - Execute the phishing campaign which may include communication containing:
    - Messages designed to convince the user to open files, click links, or perform generic actions on behalf of the tester
    - Links to attacker controlled web sites
    - Attachments and files containing pseudo malware
    - Links to web-sites that mimic legitimate corporate web-sites designed to harvest credentials
    - Links to web forms requesting the user submit sensitive data
    - Impersonated identities of trusted individuals
  - Monitor and record user responses.

- *Voice Based Social Engineering*
  - Identify highly exposed phone numbers or voice end-points using Open Source Intelligence (OSINT) methods.
  - Attempt impersonation of Customer-trusted identities which may include Customer's customers, employees, and vendors.
  - Attempt to solicit the individual to provide sensitive information such as:
    - Access credentials
    - Confidential information
    - Financial data
    - Personally Identifiable Information of customers or other employees
    - Customer-defined sensitive information
  - Attempt to convince personnel to perform actions on behalf of the caller.
  - Document successful social engineering attempts.
  - Provide the Social Engineering Report to Customer for review and approval.

Specific Service Responsibilities of Customer

- *E-mail Based Social Engineering*
  - Provide a listing of target names and e-mail addresses.
  - Approve e-mail addresses identified during intelligence gathering as targets.
  - Approve social engineering scenarios, when required.
  - Configure e-mail servers, gateways, and filters to accept mails from the Cisco testing e-mail server irrespective of transmission rate or content.
  - Ensure individuals that should not receive phishing e-mails are clearly identified.
  - Provide information regarding which targets reported social engineering attempts, when required.

- *Voice Based Social Engineering*
  - Provide a listing of target names and phone numbers.

- Approve phone numbers identified during intelligence gathering as targets.
- Approve social engineering scenarios, when required.
- Ensure individuals that should not receive phone calls are clearly identified.
- Provide information regarding which targets reported social engineering attempts, when required.
- Review and approve the Social Engineering Report.

Red Team

Cisco will perform a focused Red Team test of the Customer. The primary objective of the test is to gain access to valuable systems and data. The testing will attempt to exercise security monitoring and response capabilities and provide an opportunity to measure the effectiveness of security investments against a simulated threat. The engagement will be restricted to remote attack vectors (e.g., direct attacks against Customer computers and users exposed on the Internet).

Specific Service Responsibilities of Cisco

- Perform intelligence gathering as follows:
  - Electronic asset information gathering – scouring online repositories for the following:
    - Online assets associated with the organization, including but not limited to:
    - Owned or co-owned IP blocks
    - Registration and ownership information cross-references with known assets
    - Identification of domains & sub-domains
    - Identification of subsidiaries
    - Perform perimeter scans of live services
    - Identify used operating systems, and other technologies
    - Identify security defenses to be circumvented
    - Identification of technologies in use
    - Construct a view of the attack surface
  - Personnel information gathering
    - Discover employee emails openly available online
    - Gather employee names from social media
    - Generation of email database based on gathered information
- Perform Threat modeling, vulnerability discovery, and attack surface analysis as follows:
  - Exploitation activities on vulnerable environments identified during digital profiling or as provided by the Customer
  - Exploit design and architectural weaknesses
  - Compromise system components by exploiting implementation weaknesses in software through buffer overflows, remote code execution, cross-site scripting, SQL injection, and other attacks
  - Test operational weaknesses within patch management, configuration management, and system deployment practices
  - Exploit user weaknesses through password guessing and password cracking attacks
  - Circumvent security controls by evading firewalls, intrusion detection systems, anti-virus, access controls, cryptographic protections, and data loss prevention systems
- Post-exploitation activities within the exploited environments
  - Leverage established beach-heads within the organization to establish persistence
  - Leverage established beach-heads within the organization to escalate privileges
  - Search for credentials and sensitive data (e.g., personally identifiable information, credit card numbers)

Specific Service Responsibilities of Customer

- Provide Cisco with access to key individuals for technical questions.
- Provide Cisco with access to key individuals in case the need arises, such as unexpected behavior resulting from this assessment.
- Provide Cisco with available window of hours for testing.
- Provide Cisco with approval to conduct testing and automated scanning on environments within scope of this engagement (obtained from Digital Profile or provided by the customer)
- Allow Cisco equipment and tools to be placed on and used against the target environment.
- Review and approve the Red Team Document.

Mobile Security Strategy Workshop

Specific Service Responsibilities of Cisco

- Using the Cisco Mobile Security Framework, conduct a single, multi-day workshop with Customer to identify mobile business opportunities, educate on mobile security, and facilitate an assessment of current capability to holistically address all facets of

mobile security.
- Develop a recommended future state based on business priorities.
- Develop a roadmap of initiatives over time to reach target state.
- Develop Mobile Security Strategy report to document findings and recommendations.
- Provide an executive summary presentation

Specific Service Responsibilities of Customer
- Provide access to the appropriate resources with knowledge and authority to work with Cisco during the assessment workshop.
- Designate person(s) from within its organization to serve as a liaison to Cisco
- Provide reasonable electronic access to Customer's Network and security devices to enable Cisco during the workshop meetings.

Cloud Security Strategy Workshop

Specific Service Responsibilities of Cisco
- Using the Cisco Cloud Security Framework, conduct a single, multi-day workshop with Customer to educate on cloud security and facilitate an assessment of current capability to holistically address all facets of cloud security.
- Develop a recommended future state based on business priorities.
- Develop a roadmap of initiatives over time to reach target state.
- Develop Cloud Security Strategy report to document findings and recommendations.
- Provide an executive summary presentation

Specific Service Responsibilities of Customer
- Provide access to the appropriate resources with knowledge and authority to work with Cisco during the assessment workshop.
- Designate person(s) from within its organization to serve as a liaison to Cisco
- Provide reasonable electronic access to Customer's Network and security devices to enable Cisco during the workshop meetings.

Cloud Compliance Health Check

Specific Service Responsibilities of Cisco
- Using a common security compliance control framework or a single customer requirement (such as PCI, HIPAA, etc.) review a single cloud environment for potential compliance issues and gaps.
- Using the common compliance framework, findings will be mapped to Customer regulatory and legal requirements relating to information security.
- Standard delivery maps to one country’s requirements, if other jurisdictions are required, 24 hours will be added per jurisdiction.
- Develop Cloud Compliance Health report to document findings and recommendations.
- Provide an executive summary presentation

Specific Service Responsibilities of Customer
- Provide access to the appropriate resources with knowledge and authority to work with Cisco during the assessment workshop.
- Designate person(s) from within its organization to serve as a liaison to Cisco
- Provide reasonable electronic access to Customer's Network and security devices to enable Cisco during the workshop meetings.

Cloud Architecture Assessment

Specific Service Responsibilities of Cisco
- Perform a security architecture review of one of the Customer's cloud environment, through white boarding sessions, interviews and documentation reviews.
- Review areas like identity and access management, authorization, isolation, network connectivity, orchestration, resiliency, encryption, and monitoring.
- Identify and document the potential architecture/design weakness.
- Develop Cloud Architecture Assessment report to document findings and recommendations.
- Provide an executive summary presentation.

Specific Service Responsibilities of Customer

- Provide access to the appropriate resources with knowledge and authority to work with Cisco during the assessment workshop.
- Designate person(s) from within its organization to serve as a liaison to Cisco
- Provide reasonable electronic access to Customer's Network and security devices to enable Cisco during the workshop meetings.

Security Metrics Workshop

Specific Service Responsibilities of Cisco

- Perform a workshop with customer and identify key security questions and metrics that need to be answered and reported on regular basis.
- Develop a custom metrics dashboard to use in the regular reporting of the identified metrics.
- Provide recommended calculation methodology, thresholds, and dependencies as well as a roadmap for metrics maturity if the recommended metrics cannot be currently collected.
- Develop Security Metrics Workshop report to document findings and recommendations.
- Provide a sample dashboard

Specific Service Responsibilities of Customer

- Provide access to the appropriate resources with knowledge and authority to work with Cisco during the assessment workshop.
- Designate person(s) from within its organization to serve as a liaison to Cisco
- Provide reasonable electronic access to Customer's Network and security devices to enable Cisco during the workshop meetings.

Third Party Assessment

Specific Service Responsibilities of Cisco

- Cisco will review Customer's vendor or a selected 3rd party's security program for potential security weakness that may result in risks to Customer.
- The assessment may include one of the following
    - Provide one full onsite risk assessment at one third party vendor environment.
    - Provide two onsite rapid ISO 27002 health checks at different third parties.
    - Provide two remote lightweight risk assessments against different third parties.
- Develop Third Party Assessment report to document findings and recommendations.

Specific Service Responsibilities of Customer

- Obtain necessary approvals and access to enable Cisco to perform assessment of identified vendor or third party(s).
- Provide access to the appropriate resources with knowledge and authority to work with Cisco during the assessment workshop.
- Designate person(s) from within its organization to serve as a liaison to Cisco
- Provide reasonable electronic access to Customer's Network and security devices to enable Cisco during the workshop meetings.

Privacy Impact Analysis

Specific Service Responsibilities of Cisco

- Using the Cisco Privacy Framework, Cisco will conduct a two-day workshop to understand the business requirements, issues, obligations and possible approaches to compliance for processing Personally Identifiable Information (PII) within a specific business or technology initiative and perform a review of current capabilities.
- Develop a customized set of privacy requirements and maturity goals as per the business requirement and relevant privacy obligations in support of the target business initiative.
- Develop a roadmap for implementing the responsible information management practices.
- Provide recommendations for compliance assurance testing.
- Provide a Private Impact Analysis report and executive presentation.

Specific Service Responsibilities of Customer

- Provide access to the appropriate resources with knowledge and authority to work with Cisco during the assessment workshop.
- Designate person(s) from within its organization to serve as a liaison to Cisco
- Provide reasonable electronic access to Customer's Network and security devices to enable Cisco during the workshop meetings.

Security/IT Risk Program Support Staff Augmentation

Specific Service Responsibilities of Cisco

- Cisco to provide information security leaders (which could be Senior Consultants or Managers or Senior Managers) in staff augmentation roles to support/lead Customer's security programs and initiatives. The duration of this support will be 6 weeks.

Specific Service Responsibilities of the Customer

- Provide Cisco with details around what type of support is needed when a request is made.

Information Security Program Development

During this engagement, Cisco will perform an assessment of Customer's IT risk assessment processes and program attempting to identify, as applicable, areas for program enhancement or improvement.

Specific Service Responsibilities of the Cisco

- Determine Customer's IT Risk context, including the following:
    a. External Requirements
        - Gather input from Customer's risk management, compliance and legal representatives to identify external obligations concerning IT risk management
    b. Internal Requirements
        - Document IT and business stakeholder expectations and success factors for IT risk
        - Document unsatisfactory perceptions of current process
    c. Operational Risk Management
        - Gain an understanding of the role IT risk plays within the organization's operational risk framework and enterprise risk management strategy
    d. Organization and Culture within IT
        - Interview IT stakeholders and staff attempting to identify cultural factors that influence risk identification
    e. Review the Customer's current IT Risk assessment approach, activities and feedback, and compare to expectations
    f. Current IT Risk Process Review
        - Review IT risk organizational structure, team count, and field of view
        - Review process documentation
        - Review how automation is used
        - Investigate execution effectiveness from responsible individual(s)
        - Identify input and perception of process from contributors via interviews
        - Reporting and Measurements
            - Review IT risk assessment reporting
            - Investigate actionable outcomes and organizational responses to IT risk assessment findings
- Document detailed findings and recommendations in the Summary Findings and Recommendations Report.
- Conduct an executive summary presentation of recommendations to Customer's leadership team.

Specific Service Responsibilities of the Customer

- Identify a project sponsor with responsibility for completion of the project and with the authority to make decisions concerning execution of the project.
- Provide a Customer project manager to schedule stakeholder meetings and fulfill information requests.
- Provide access to key individuals for interviews and questions.
- Provide Cisco with findings from any recent IT risk assessments.
- Provide Cisco with access to any IT risk related policies and other relevant IT risk operational documentation.

Information Security Risk Program Development

During this engagement, Cisco will perform an assessment of Customer's IT risk assessment processes and program attempting to identify, as applicable, areas for program enhancement or improvement.

Specific Service Responsibilities of the Cisco

- Determine Customer's IT Risk context, including the following:
    a. External Requirements

        - Gather input from Customer's risk management, compliance and legal representatives to identify external obligations concerning IT risk management
    b. Internal Requirements
        - Document IT and business stakeholder expectations and success factors for IT risk
        - Document unsatisfactory perceptions of current process
    c. Operational Risk Management
        - Gain an understanding of the role IT risk plays within the organization's operational risk framework and enterprise risk management strategy
    d. Organization and Culture within IT
        - Interview IT stakeholders and staff attempting to identify cultural factors that influence risk identification
    e. Review the Customer's current IT Risk assessment approach, activities and feedback, and compare to expectations
    f. Current IT Risk Process Review
        - Review IT risk organizational structure, team count, and field of view
        - Review process documentation
        - Review how automation is used
        - Investigate execution effectiveness from responsible individual(s)
        - Identify input and perception of process from contributors via interviews
        - Reporting and Measurements
            - Review IT risk assessment reporting
            - Investigate actionable outcomes and organizational responses to IT risk assessment findings
- Document detailed findings and recommendations in the Summary Findings and Recommendations Report.
- Conduct an executive summary presentation of recommendations to Customer's leadership team.

Specific Service Responsibilities of the Customer

- Identify a project sponsor with responsibility for completion of the project and with the authority to make decisions concerning execution of the project.
- Provide a Customer project manager to schedule stakeholder meetings and fulfill information requests.
- Provide access to key individuals for interviews and questions.
- Provide Cisco with findings from any recent IT risk assessments.
- Provide Cisco with access to any IT risk related policies and other relevant IT risk operational documentation.

Information Security Risk Assessment

Cisco will conduct an Information Security Risk Assessment to identify, assess, and recommend mitigation for strategic and operational security risks that may affect the Customer's business. The risk assessment reviews business and IT strategies and determines business-relevant information security risks threatening achievement of defined strategies. The assessment will seek to identify critical risks through a mix of strategic analysis, documentation review, interviews, control observations, and facilitated risk assessment. The risk assessment evaluates current risk controls and seeks to determine the residual risk. Based on business priorities and Cisco' understanding of risk tolerance gained through executive interviews, we will develop a custom information security risk profile and remediation roadmap.

Specific Service Responsibilities of the Cisco

- Gain understanding of the business context and customize the Risk Assessment:
    a. Interview key IT and business stakeholders to allow for understanding of business and technology strategies, objectives and other key critical dependencies on IT
    b. Identify critical business processes and their known application dependencies (This applies only if going to business process or asset level analysis – so only for deep risk assessments, otherwise take out.)
    c. Review entity level risk controls and governance processes
    d. Formalize and agree on information security risk tolerance and business relevant risk rating criteria
- Analyze key strategic trends; the strategic analysis will take into account:
    a. Business strategies, customer expectations, and relevant industry trends identified by stakeholders
    b. Relevant technology strategies
    c. Regulatory and legal trends
    d. Relevant information security and external threat trends
- Review and attempt to identify information security risks within business processes, and the IT architecture, infrastructure and operational processes that support critical IT assets. This includes identifying potential risks and examining current controls, via:
    a. Review of findings from previously performed information security risk assessments
    b. Review of available information security policies, standards, and procedures
    c. Review of relevant business process and IT operational process documentation

d. Facilitation of a group risk assessment workshops with a subset of stakeholders to surface and assess risks based on informal institutional knowledge
e. Interviews with key stakeholders and subject matter experts
f. Review of architecture and support documentation
g. Analysis of past audit results
h. Review of available risk sources, such as problem and incident management reports and IT performance metrics
i. Areas of analysis may include, where relevant:
    a) Information security governance and oversight
    b) Information security policies, standards, and procedures
    c) Information classification and handling
    d) Compliance processes
    e) Risk assessment and management
    f) Enterprise security architecture
    g) Security metrics, measurement, and performance management
    h) Awareness and education
    i) Vulnerability, patch, change, and asset management
    j) Security monitoring and instrumentation
    k) Incident management
    l) Software acquisition, development, and maintenance
    m) System resiliency and disaster recovery
    n) 3rd party risk management
    o) Identity and access management
    p) Human resources security
    q) Physical and environmental security
    r) Network security
    s) System security
    t) Data security and encryption
    u) Mobile devices and media security
    v) Malicious code protection

- Assess risks:
    a. Aggregate and analyze potential risks based on the type of impact
    b. Assess identified risks, ranking each for probability that the risk will materialize and the potential impact if it should occur.
    c. Review assessed risks against customized risk rating criteria in order to prioritize them and determine those that require action
- Develop a remediation roadmap to include:
    a. Recommended risk treatment options
    b. Recommended improvements that maps initiatives over a pre-determined time frame
- Provide Customer with the Information Security Risk Assessment Report.

Specific Service Responsibilities of the Customer

- Identify a project sponsor with responsibility for completion of the project and with the authority to make decisions concerning execution of the project.
- Provide a Customer project manager to schedule stakeholder meetings and fulfill information requests.
- Ensure appropriate business and IT stakeholders participate in the review and acceptance of project work products and deliverables.
- Provide requested documentation including, but not limited to, risk management and information security policies, standards, and procedures, business and IT process documentation, disaster recovery and incident response plans, system and infrastructure configurations, third party contracts, and management reporting.
- Provide Cisco with appropriate building access and badges, workspace, meeting space, telephone and LAN access for team members.

Security Metrics Program Development

Cisco will assist Customer in developing a comprehensive security metrics program, including analysis and creation of an initial security metrics catalog based on Customer needs and requirements.

Cisco will leverage recognized standards for security measurement and metrics, including ISO *27004: Information Technology – Security Techniques – Information Security Management – Measurement*. Cisco uses a combination of approaches to deliver a Security Metrics Program Development engagement including educational workshops, individual and group working sessions, and

review of artifacts. The resulting deliverable will include recommendations for strategic and tactical improvement of the measurement program, as well as specific metrics developed over the course of delivery.

Specific Service Responsibilities of the Cisco

- Review the maturity of the Customer's existing IT and Information Security Measurement Program
- Facilitate introductory security metrics workshops with business and technical resources, which will:
  a) Provide an overview of measurement in industry
  b) Provide an overview of specific measurement applications in information and IT security
  c) Provide an overview of ISO 27004 and other appropriate security measurement standards and frameworks
  d) Explain the Goal-Question-Metric (GQM) methodology
  e) Discuss specific security measurement examples and case studies
- Analyze workshop results and applicability to the overall engagement
- Assess and review existing security measurement program capabilities, maturity and processes
  a) Interview stakeholders
  b) Review program documentation and artifacts
  c) Compare existing program to recommendations and requirements of ISO 27004, and other measurement frameworks
  d) Share initial results with Customer stakeholders
- Facilitate GQM workshops with business and technical resources for purposes of developing and improving the Customer's metrics catalog.
  a) Provide detailed education on GQM methodology
  b) Use GQM techniques to define and explore specific strategic measurement scenarios for new or existing Customer security metrics
  c) Analyze GQM results and incorporate them into the metrics catalog

- Provide Customer with the Security Metrics Program Development Report and conduct an executive summary presentation

Specific Service Responsibilities of the Customer

- Identify a project sponsor with responsibility for completion of the project and with the authority to make decisions concerning execution of the project.
- Provide a Customer project manager to schedule stakeholder meetings and fulfill information requests.
- Ensure appropriate business and IT stakeholders participate with Cisco in review and acceptance of project deliverables.
- Provide access to requested documentation including current security metrics, operational processes, and management dashboards.
- Work with Cisco to schedule workshop(s); and ensure availability of stakeholders.
- Provide Cisco with access to appropriate building access and badges, workspace, meeting space, telephone and LAN access for team members.

Third Party Risk Program Development

Cisco will conduct an assessment of Customer's Vendor and Third-party Risk Management Program. The assessment will review program processes to assess effectiveness in identifying, treating, governing, and monitoring third-party risks.

The assessment covers the entire lifecycle of third-party engagements including requirements development, due diligence and selection, negotiation, transition and transformation, steady state operations and termination. Identified issues will be prioritized based on risk and reported. Actionable recommendations will be provided with a proposed improvement plan.

Specific Service Responsibilities of the Cisco

- Review the context of the Third-party Risk Management Program
- Review key business strategies, objectives and initiatives dependent on third-parties and related elements of overall strategy
- Identify critical third-party relationships, services, technologies and products and how they support Customer's business processes
- Define overall risk tolerance and formalize business relevant risk rating criteria
- Review third-party risk management processes and identify potential issues
- Identify relevant governance, procurement, due diligence, relationship management, assurance and risk management processes
- Refine understanding of the Customer's interaction with third-parties

- Review process documentation and interview key stakeholders to identify potential issues based on business requirements and best practice models. Areas of analysis may include, as appropriate:
    1. Third-party inventory
    2. Prioritization
    3. Requirements development
    4. Risk assessment
    5. Business continuity planning
    6. Risk based requirements
    7. SLA definition
    8. Contract standards and templates
    9. Negotiation input and impact analysis
    10. Due diligence procedures
    11. Transition and transformation management
    12. Performance monitoring
    13. Security and compliance assurance processes
    14. Governance structures, oversight, and accountability mechanisms
- Evaluate Sample Relationships
    1. Validate customer requirements
    2. Identify a sample of third-party relationships based on client prioritization and risk
    3. Perform a high-level assessment against requirements attempting to identify risks and determine how they are being identified, managed and monitored; the purpose of this assessment is to validate previous findings and identify new issues due to execution quality
    4. The assessment will be based upon an interview with key internal stakeholders and third-party representatives, and will include:
        - Information governance and protection
        - Compliance requirements
        - Operational expectations
        - Business continuity and operational resilience
        - Change management
- Assess Risks
    1. Based on business risk tolerance and agreed risk assessment criteria, assess and prioritize risks
    2. Define risk profile
- Develop Third-party Risk Management Program Improvement Roadmap
    1. Based on prioritized risks, develop an improvement roadmap including actionable improvement recommendations and tangible interim states
    2. To the extent possible, estimate cost, time and resources required to implement improvement roadmap
- Provide Customer with the Third-party Risk Management Program Assessment Report and the Executive Summary.

Specific Service Responsibilities of the Customer

- Identify a project sponsor with responsibility for completion of the project and with the authority to make decisions concerning execution of the project.
- Provide a Customer project manager to schedule stakeholder meetings, fulfill information requests, and manage third-party interaction.
- Ensure appropriate business and IT stakeholders participate with Cisco in review and acceptance of project deliverables.
- Provide access to appropriate Third-party resources; successful completion of this project will require active participation and timely review from Third-party.
- Ensure timely provision of requested documentation from Customer and Third-party.
- Provide Cisco with access to appropriate building access and badges, workspace, meeting space, telephone and LAN access for team members.

Assessment of Organizational Alignment to ISO 27001

Cisco understands that Customer is considering the attainment of ISO 27001:2013 (hereafter, ISO 27001) certification in the future and would like advisory services support to understand the process and evaluate their general state of preparedness for certification. The goal of this project is to provide an overview of the ISO 27001 certification process, assist in the definition of a potential scope for ISO 27001 certification, and to provide a high-level assessment of process and control alignment to the standard to determine Customer's current level of preparedness.

Cisco will perform an assessment of Customer's current alignment to the ISO27001 standard, including Annex A, and the controls

covered by ISO 27002:2013. The assessment will consist of documentation reviews and interviews to determine current alignment to ISO control requirements. Cisco will provide recommendations and a roadmap for preparation for ISO 27001 certification.

Specific Service Responsibilities of the Cisco

- Provide a half-day workshop with key stakeholders to provide an overview of the ISO 27001 standard and the general process required to attain certification
- Work with Customer to review scope options and define the proposed scope for ISO certification
  a) Review business and information security goals
  b) Interview key stakeholders to review information security strategies and how they relate to business objectives
  c) Outline the in-scope processes, supporting systems, and support teams
  d) Determine if any Annex A controls may be deemed out of scope
- Perform high-level assessment of current alignment with ISO requirements:
  a) For ISO 27001
    - Review the security architecture at a high-level
    - Review relevant security governance processes
    - Review information security charter, policy, and other associated documentation
    - Review the ISO 27001 mandatory documents and mandatory records
    - Review risk management methodology and the most recent information security risk assessment documentation
    - Interview information security officer and senior management, as needed, to assess practices and adherence to defined objectives
    - Document findings and gaps
- Develop recommendations to address gaps and a roadmap outlining recommended priority.
- Provide an executive presentation of assessment findings

Specific Service Responsibilities of the Customer

- Identify a project sponsor with responsibility for completion of the project and with the authority to make decisions concerning execution of the project.
- Provide a Customer project manager to schedule stakeholder meetings and fulfill information requests.
- Ensure appropriate business and IT stakeholders participate with Cisco in review and acceptance of project deliverables.
- Provide access to available documentation including: company business goals and strategies; existing IT and security strategy, policies, and procedures; any relevant regulatory considerations; previous security or audit assessments.
- Provide Cisco with access to appropriate building access and badges, workspace, meeting space, telephone and LAN access for team members.
- Provide ISO related documentation, including, if available:
  - Mandatory ISO 27001Documents:
    - Scope of the ISMS
    - Information security policy and objectives
    - Risk assessment and risk treatment methodology
    - Statement of Applicability
    - Risk treatment plan
    - Risk assessment report
    - Definition of security roles and responsibilities
    - Inventory of assets
    - Acceptable use of assets
    - Access control policy
    - Operating procedures for IT management
    - Secure system engineering principles
    - Supplier security policy
    - Incident management procedure
    - Business continuity procedures
    - Statutory, regulatory, and contractual requirements
  - Mandatory records:
    - Records of training, skills, experience and qualifications
    - Monitoring and measurement results
    - Internal audit program
    - Results of internal audits
    - Results of the management review
    - Results of corrective actions

- Logs of user activities, exceptions, and security events
- Non-mandatory, yet commonly found documents:
  - Procedure for document control
  - Controls for managing records
  - Procedure for internal audit
  - Procedure for corrective action
  - Bring your own device (BYOD) policy
  - Mobile device and teleworking policy
  - Information classification policy
  - Password policy
  - Disposal and destruction policy
  - Procedures for working in secure areas
  - Clear desk and clear screen policy
  - Change management policy
  - Backup policy
  - Information transfer policy
  - Business impact analysis
  - Exercising and testing plan
  - Maintenance and review plan
  - Business continuity strategy

Assessment of Organizational Alignment to ISO 27002

Cisco will perform a security assessment intended to determine adherence to each domain of the ISO 27002:2013 standard. The assessment will consist of documentation reviews and interviews to determine control selection and design effectiveness. Cisco will also

provide an assessment of the operational effectiveness of controls by performing high-level effectiveness reviews of sample controls, and physical site reviews of data centers and IT operations. Cisco will prioritize and map recommendations to provide an ISO 27002 roadmap.

Specific Service Responsibilities of Cisco

- Review the organization and information security goals.
- Review the information security organization structure.
  - Interview key stakeholders to understand information security strategies and how they relate to business objectives
  - Gain a high-level understanding of the security architecture
  - Review relevant security governance processes
- Identify appropriate stakeholders for the interview phase of the assessment.
- Review documentation, including:
  - Most recent information security risk assessment
  - Information security policies and standards
  - Control documentation for appropriate control selection and design based on ISO 27002
- Identify ISO 27002 gaps in terms of information security risk assessment, control selection, and documented design.
- Interview stakeholders using ISO 27002 questionnaire; interviews will be performed to:
  - Validate control design documentation
  - Understand known gaps and assess the operational effectiveness of controls
  - Understand undocumented control processes
  - Determine potential systemic risks within IT operations
- Perform high level effectiveness reviews against sample controls via one of two methods:
  - Review evidence of control execution and completion
  - Observe the control in operation
- Perform a physical site review of data centers and IT operations to observe implemented controls.
- Document findings, including identified gaps and issues, remediation recommendations in the ISO 27002 Assessment Report.
- Provide Customer with the ISO 27002 Assessment Report and Executive Summary.

Specific Service Responsibilities of Customer

- Identify a project sponsor with responsibility for completion of the project and with the authority to make decisions concerning execution of the project.
- Provide a Customer project manager to schedule stakeholder meetings and fulfill information requests.
- Ensure appropriate business and IT stakeholders participate with Cisco in review and acceptance of project deliverables.
- Provide access to available documentation including: company business goals and strategies; existing IT and security strategy, policies, and procedures; any relevant regulatory considerations; previous security or audit assessments.
- Provide Cisco with access to appropriate building access and badges, workspace, meeting space, telephone and LAN access for team members.

HIPAA and HITECH Assessment

Cisco will perform a HIPAA/HITECH Readiness Assessment to determine adherence to the requirements of the Health Insurance Portability and Accountability Act ("HIPAA") security rule, with the additional relevant requirements of the Health Information Technology for Economic and Clinical Health ("HITECH") Act. The assessment will consist of documentation reviews and interviews to determine control selection and design effectiveness. Cisco will prioritize findings and map remediation efforts to provide a HIPAA Security Readiness Roadmap.

Specific Service Responsibilities of Cisco

- Review the Customer's organizational structure, business drivers, regulatory environment, and information security goals:
  - Review the information security organizational structure
  - Interview key stakeholders to understand information security strategies and how they relate to business objectives
  - Review security architecture documentation
  - Review relevant security governance and internal audit processes
- Determine HIPAA/HITECH compliance:
  - Identify the business processes and transactions that use electronic protected health information (ePHI), via interviews with relevant personnel
  - Based on Customer interviews, define information asset scope boundaries by identifying relevant applications and infrastructure that store or process ePHI
- Determine physical locations that are in scope for the assessment and identify which controls apply at each location.
- Develop scope statement to define the applicability of the standard, and review with Customer.
- Identify appropriate stakeholders to participate with Cisco in the interview phase of the assessment.
- Review Customer's existing risk assessment(s), policies, and control documentation:
  - Review information security policies and standards
  - Review the most recent information security risk assessment
  - Review audit reports related to information security
  - Review control documentation for appropriate control selection and design
- Perform interviews, control effectiveness reviews, and physical site inspection; interview identified stakeholders to:
  - Validate control design documentation
  - Review operational effectiveness of controls
  - Investigate undocumented control processes or identify additional documentation available for review
- Selected sample controls that correspond to HIPAA requirements and perform operational effectiveness reviews to characterize the effectiveness of control implementation. High level effectiveness reviews will be performed against selected sample controls via one of three methods:
  - Review evidence of control execution and completion
  - Observe the control in operation
  - Review assessment of control within PCI ROC or other relevant assessment
- Perform a physical site inspection of data centers to observe implemented controls.
- Perform a physical site inspection of IT operations and management areas at corporate headquarters.
- Provide Customer with a Detailed Assessment Report outlining the findings of the assessment.
- Document identified HIPAA/HITECH security rule compliance gaps and control effectiveness issues.
- Develop remediation recommendations and adherence roadmap.
- Provide Customer with the HIPAA/HITECH Security Rule Readiness Assessment Executive Summary.

Specific Service Responsibilities of the Customer

- Identify a project sponsor with responsibility for completion of the project and with the authority to make decisions concerning execution of the project.
- Provide a Customer project manager to schedule stakeholder meetings and fulfill information requests.
- Provide access to key individuals for interviews and technical questions.
- Provide available documentation to allow Cisco to fulfil its responsibilities described herein.
- Provide access to all resources identified as within scope, for the purposes of assessment against the HIPAA guidelines.
- Provide Cisco with access to suitable office facilities for meetings, interviews, and facilitated sessions for work being conducted at the Customer's location.

PCI ASV Scanning Service

Cisco will perform four (4) external network security scans at ninety-day intervals as required by the Payment Card Industry ("PCI") Data Security Standard. Cisco will perform the security scanning on a pre-defined number of individual IP addresses.

Specific Service Responsibilities of the Cisco

- Conduct a meeting with Customer to prepare for each quarterly scan to:
  - Validate that the contact information on record is current and make corrections as needed.
  - Walk the Customer through an Asset Wizard in the Cisco Security Services Web Portal to:
    - Verify that all in-scope IP addresses necessary to maintain PCI compliance will be included in the scan
    - Determine if there are any load balancers that are in-scope for the scan and, if so, whether or not all configurations of load balanced devices are synchronized
    - Verify that all IPS/IDS technology and any other network infrastructure devices are configured so that they will not interfere with scans
  - Determine date and time for the scan and any time limitations that must be set.
- Perform the quarterly scan using the Cisco ASV scanning solution that has been approved by the PCI Security Standards Council (SSC), using scan settings as dictated by the PCI SSC
- Provide Customer with PDF Quarterly PCI ASV Executive Summary and Detail reports (External Security Scan Report) in format required by PCI SSC.
- Work with Customer to resolve PCI non-compliant vulnerabilities that the Customer feels are false positives.
- Perform up to one (1) quarterly re-scan of all IP addresses that had PCI non-compliant vulnerabilities reported after the initial quarterly scan.
- Cisco will attest and certify each quarterly scan if, and only if, Customer has provided proper evidence for any disputed false positive vulnerabilities and/or PCI non-compliant vulnerabilities detected in the initial quarterly scan have been remediated and are not reported by the re-scan.

Specific Service Responsibilities of the Customer

- Identify a project sponsor with responsibility for completion of the project and with the authority to make decisions concerning execution of the project.
- Provide a Customer project manager to schedule stakeholder meetings and fulfill information requests.
- Provide access to key individuals for interviews and technical questions.
- Provide access to all resources identified as within scope, for the purposes of assessment against the PCI Data Security Standard.
- Provide emergency contact information including name, title, e-mail, business and mobile phone numbers.
- Customer shall be responsible for:
  - Verifying and attesting that all in-scope IP addresses to maintain PCI compliance have been reported to Cisco
  - Reporting load balancers in-scope for the scan
  - Attesting that all configurations of load balanced devices are synchronized and provide evidence that the configurations are in fact synchronized, or Customer shall provide copies of detailed internal vulnerability scans performed by the Customer and that validate that there are no PCI non-compliant vulnerabilities reported
  - Configuring IPS/IDS technology and any other network infrastructure devices so that they will not interfere with any scan
- Provide a date and time for each scan and any time limitations that must be set for the scan.
- Within twenty five (25) calendar days of a quarterly scan finishing and Customer's receipt of the report:
  - Customer must remediate all PCI non-compliant vulnerabilities or provide sufficient evidence for Cisco to make a judgment on any reported false positive vulnerabilities

- Customer must generate a report and a request that Cisco attest to and certify the scan

PCI-DSS Readiness Assessment

Specific Service Responsibilities of Cisco

- This is a time-boxed assessment against the then current PCI (such as DSS 3.1) security standard performed by a Cisco.
- Provides insight to the current PCI compliance stance of one Cardholder Data Environment (CDE)
- Perform review via interviews and key documentation, to cover all PCI-DSS requirements (Note: This differs from a Report on Compliance (ROC) in that full sampling of all evidence may not be performed)
- Provide a detailed report outlining tactical and strategic remediation and recommendations
- Provide a detailed planning matrix in Microsoft Excel of remediation required.

Specific Service Responsibilities of Customer

- Provide access to the appropriate resources with knowledge and authority to work with Cisco during the assessment workshop.
- Designate person(s) from within its organization to serve as a liaison to Cisco
- Provide reasonable electronic access to Customer's Network and security devices to enable Cisco during the workshop meetings.

Enterprise Security Advisor

Specific Service Responsibilities of the Cisco

Cisco will provide a part time, technology neutral, Enterprise Security Advisor to support Customer's security strategy and planning to facilitate efficient rollout and alignment of security products and services with Customer's wider security, risk and compliance program. This service is delivered flexibly, as agreed by the parties, with the intention of enabling the Customer to better achieve business objectives. Initial delivery includes 2-4 weeks to review initiatives, in-flight projects, and security objectives, identify initial deliverables and set the cadence of ongoing meetings and communications as agreed by the parties. As the Customer environment evolves, the Security Architect will participate and support in the evolution of the corresponding security, risk and compliance programs, which may include the following main activities:

- Review and facilitate alignment of business requirements to security objectives, policies, and technology implementations.
- According to a cadence agreed by the parties, lead regular planning and status meetings to agree engagement activities, deliverables, and timelines.
- According to a cadence agreed by the parties, participate in a regular meeting concerning the portfolio of active/planned and planned projects to provide recommendations on timing, integration activities, dependencies, policy, processes and procedure requirements.
- Work with customer and other Cisco subject matter experts to support the planning and implementation of target security architecture to achieve security objectives.
- Provide oversight of high-level design production for Cisco technology in collaboration with Customer and Cisco teams and facilitate alignment to Customer's enterprise security architecture.
- Review low level designs for alignment to agreed high-level designs as well as Customer's architectural and engineering requirements. As required and agreed, assist client with production of architectural and engineering requirements.
- Support the development of policies and standards for security, risk and compliance programs as necessary to support security operations and technology improvements.
- Assist Customer in creation of business processes to appropriately manage implemented technology.
- Support and supplement the Customer with best practices, industry trends, reference materials, and expertise available through Cisco.
- Provide services through a mix of remote and onsite collaboration according to a schedule agreed by the parties.
- Support customer ad hoc requests for security architecture support according to schedules agreed by the parties.
- Provide Cisco security architect and customer with subject matter expert support, as required and as are available to be scheduled, as agreed by the parties.

Specific Service Responsibilities of the Customer

- Assign a project sponsor with the authority to make decisions concerning execution of the project.
- Assign a client project manager to schedule stakeholder meetings and fulfill information requests.
- Timely access to key individuals for interviews and technical questions.
- Timely access to available documentation, as required, which may include: company business goals and strategies; existing IT and security strategy, policies, and procedures; any relevant regulatory considerations; previous security or audit assessments.
- Agree with Cisco schedule of regular meetings as well as engagement objectives, deliverables, and timelines.
- Schedule meetings as agreed.

- Provide timely input and reviews of agreed deliverables.
- Communicate ad hoc requests for activities and deliverables in a timely manner. Customer understands and acknowledges that assigned architect is not a dedicated resource. The parties will mutually agree to ad hoc activities, timing, and deliverables.

Security Segmentation Service

Using Cisco's Security Segmentation Architecture methodology, Cisco will develop and provide a High Level Design ("HLD") for enterprise network security architecture. The HLD will define a set of segmented security architecture patterns including technical control capabilities and a logical implementation diagram for each type of segment. In support of the HLD, Cisco will provide an Application Placement Process which includes the decision-making process and criteria for determining the instantiation and application of developed design patterns. Cisco will also provide an implementation roadmap for the new architecture.

The primary methods of input from the Customer are a Security Segmentation workshop, interviews, and feedback on draft deliverables.

Specific Service Responsibilities of the Cisco

- Conduct a kick off call to introduce teams, discuss logistics, and review expectations for the onsite Security Segmentation workshop.
- Work with the Customer project manager to define required and optional stakeholders to participate in the workshop; it is expected that this will include representatives from the architecture, applications management, security, and networking teams.
- Collect and review background information and documentation related to business and technical requirements. Documentation review should include as many of the following as available: a) applicable security policies, standards, and procedures; b) data and system classification guidelines and inventories; c) Customer organizational structure; d) business critical assets; e) primary known threats to critical business assets; f) physical and logical network topology diagrams; g) network architecture descriptions; h) services that traverse the network; i) applications and services running over the network; j) high-level architecture of data center, internal servers, user host connectivity and Internet connectivity; k) network management system architecture; and l) relevant and recent security assessments or strategy documentation completed by third parties or Customer.
- Schedule initial interviews and review sessions prior to conducting the onsite workshop.
- Distribute pre-workshop questionnaires to workshop attendees.
- Provide workshop and interview agenda to Customer.
- Review Customer provided documentation and data.
- Perform one-on-one or team interviews of key stakeholders to gather information prior to the workshop, as required.

- Prepare workshop materials.
- Facilitate the onsite Security Segmentation Workshop. Workshop agenda will be designed to gain Customer input on current state architecture, business and technology drivers, and decision parameters for Security Segmentation and target state architecture.
- Create and provide a summary presentation of initial Workshop results.
- Conduct follow up interviews or request and review additional documentation from Customer.
- Develop segment creation and asset placement guidelines.
- Create and document the recommended segment definitions and design templates that include high level logical diagrams, including recommended security controls.
- Define additional recommendations concerning segment prioritization, security control implementation, and high level data flow between segments.
- Document a single cross-reference to a common industry security standard which the parties agree is relevant (e.g. NIST 800-53, PCI-DSS, or ISO 27001).
- Regularly review draft designs with Customer to enable early feedback.
- Create the HLD which includes: a) executive summary; b) high level design with recommended segments and associated controls; c) application placement process.
- Provide the HLD to Customer for review and approval.
- Define high level work breakdown structure to delineate projects or work-streams required to achieve recommended HLD.
- Collaborate with Customer to map work required onto a time line.
- Collaborate with Customer to develop an estimated level of effort or Rough Order of Magnitude to implement HLD.
- Create the Strategic Security Segmentation Roadmap and provide to Customer for review and approval.
- Conduct a final executive summary presentation summarizing recommendations, HLD, and Strategic Security Segmentation Roadmap.

Specific Service Responsibilities of the Customer

- Work with Cisco to schedule the workshops and ensure availability of stakeholders.
- Provide Cisco with access to appropriate building access and badges, workspace, meeting space, telephone and LAN access for team members.
- Identify and secure attendance of key stakeholders for the Security Segmentation workshop.

- Review the agenda for the workshop and provide feedback.
- Unless otherwise agreed to by the parties, Customer shall respond within three (3) Business Days of Cisco's request for supplementary documentation or information requests.
- Provide Cisco with the proper security clearances and/or escorts as required to access Customer's facility.
- Provide adequate facilities to conduct interviews and the workshop, including: appropriate power, desk space, audio-visual equipment, projectors or monitors, whiteboards, and at least one blank flip chart.
- Provide Cisco with access to wireless guest networks that have access to the Internet, if present in the facility.
- Supply Cisco with the workplace policies, conditions and environment in effect at Customer's facility.
- Provide feedback to Cisco as requested regarding designs within conference calls or via written request within two (2) Business Days.
- Review and approve the HLD in accordance.
- Collaborate interactively with Cisco to define work breakdown structure, timelines, and effort estimates.
- Review and approve the Strategic Security Segmentation Roadmap.
- Coordinate the scheduling of appropriate senior business and technology stakeholders to attend executive summary presentation.
- Provide adequate facilities to conduct the executive summary presentation including appropriate power, audio-visual equipment, and projectors or monitors.
- Ensure that key Customer stakeholders attend Cisco's final executive summary presentation.

Appendix-A
Service SKUs

The following list of Service Work Items (Delivery Tags) for Integration and Advisory services is provided for reference:

Integration Deliverables and Tags

Deliverables	Work Items	
Network Device Security Assessment (NDSA)	OPT-SOS-NDSA	OPT-RS NOS-NDSA
Security Advanced Change Support (Security Advanced CS)	OPT-SOS-ACS	OPT-SO NOS-ACS
Security Change Support (Security CS)	OPT-SOS-CS	OPT-SO NOS-CS
Security Cyber Range (Security CR3)	OPT-SOS-CR3	OPT-SO NOS-CR3
Security Cyber Range (Security CR5)	OPT-SOS-CR5	OPT-SO NOS-CR5
Security Design Development Support (Security DDS)	OPT-SOS-DDS	OPT-SO NOS-DDS
Security Design Review and Support (Security DRS)	OPT-SOS-DRS	OPT-SO NOS-DR
Security Health Check (Security HC)	OPT-SOS-HC	OPT-SO NOS-HC
Security Issue Resolution and Planning Support (Security IRPS)	OPT-SOS-ISUPP	OPT-SO NOS-ISUPP
Security Kick-Start Support (SKSS)	OPT-SOS-KICK	OPT-SO NOS-KICK
Security Network Consulting Support (Security NCS)	OPT-SOS-NCS	OPT-SO NOS-NCS
Security Ongoing Flexible Support (Security OFS)	OPT-SOS-OFS	OPT-SO NOS-OFS
Security Performance Tuning Support (Security PTS)	OPT-SOS-PTS	OPT-SO NOS-PTS
Security Proactive Software Recommendations (Security PSR)	OPT-SOS-PSR	OPT-SO NOS-PSR
Security Strategy and Planning Support (SSPS)	OPT-SOS-SPS	OPT-SO NOS-SPS
Security Technology Readiness Assessment (STRA)	OPT-SOS-TRA	OPT-SO NOS-TRA
Security Validation and Testing Premier Support (Security VTPS)	OPT-SOS-PVTS	OPT-SO NOS-VTPS
Security Validation and Testing Support (Security VTS)	OPT-SOS-VTS	OPT-SO NOS-VTS
Software Security Alert (SSA)	OPT-SOS-SA	OPT-SO NOS-SSA

Security Knowledge Service (Security KS)	OPT-SOS-KS	OPT-SO NOS-SMKS
Security Remote Knowledge Transfer (Security RKT)	OPT-SOS-KTM	OPT-SO NOS-RKT

Advisory Deliverables & Tags

Deliverables	Work Items	
Incident Response Retainer	OPT-SOS ADV IR	OPT-SO NOS-ADV IR
On-going Flexible Support	OPT-SOS ADV OFS	OPT-SO NOS-ADV OFS
Advisory Project Management	OPT-SOS ADV PM	OPT-SO NOS-ADV PM
Security Consulting Services		
Security Program Assessment and Strategic Roadmap	OPT-SOS ADV-SCS PASR	OPT-SO NOS-ASCS PASR
Commercial Security Program and Control Design Assessment	OPT-SOS ADV-SCS PCDA	OPT-SO NOS-ASCS PCDA
Mobile Security Strategy Workshop	OPT-SOS ADV-SCS MSW	OPT-SO NOS-ASCS MSW
Cloud Security Strategy Workshop	OPT-SOS ADV-SCS CSW	OPT-SO NOS-ASCS CSW
Cloud Compliance Health Check	OPT-SOS ADV-SCS CCHC	OPT-SO NOS-ASCS CCHC
Cloud Architecture Assessment	OPT-SOS ADV-SCS CAA	OPT-SO NOS-ASCS CAA
PCI-DSS Readiness Assessment	OPT-SOS ADV-SCS PIRA	OPT-SO NOS-ASCS PIRA
Security Metrics Workshop	OPT-SOS ADV-SCS SMW	OPT-SO NOS-ASCS SMW
Security Third Party Assessment	OPT-SOS ADV-SCS TPA	OPT-SO NOS-ASCS TPA
Privacy Impact Analysis	OPT-SOS ADV-SCS PIA	OPT-SO NOS-ASCS PIA
Security Risk Program Support Staff Augmentation	OPT-SOS ADV-SCS PSSA	OPT-SO NOS-ASCS PSSA
Application Architecture Assessment	OPT-SOS ADV-SCS AAA	OPT-SO NOS-ASCS AAA
Application Penetration Assessment	OPT-SOS ADV-SCS APA	OPT-SO NOS-ASCS APA
SDLC Improvement	OPT-SOS ADV-SCS SDLC	OPT-SO NOS-ASCS SDLC
Mobile Application Assessment	OPT-SOS ADV-SCS MAA	OPT-SO NOS-ASCS MAA
Network Architecture Assessment	OPT-SOS ADV-SCS NAA	OPT-SO NOS-ASCS NAA
Network Penetration Test	OPT-SOS ADV-SCS NPT	OPT-SO NOS-ASCS NPT
Wireless Security Assessment	OPT-SOS ADV-SCS WSA	OPT-SO NOS-ASCS WSA
Physical Security Assessment	OPT-SOS ADV-SCS PSA	OPT-SO NOS-ASCS PSA
Social Engineering	OPT-SOS ADV-SCS SE	OPT-SO NOS-ASCS SE
Red Team	OPT-SOS ADV-SCS RTBT	OPT-SO NOS-ASCS RTBT
Program Development	OPT-SOS ADV-SCS PD	OPT-SO NOS-ASCS PD
Risk Program Development	OPT-SOS ADV-SCS RPD	OPT-SO NOS-ASCS RPD
IT Risk Assessment	OPT-SOS ADV-SCS ITRA	OPT-SO NOS-ASCS ITRA
Assessment of Organizational Alignment to ISO 27001	OPT-SOS ADV-SCS OAI	OPT-SO NOS-ASCS OAI
Security and Risk Metrics Support	OPT-SOS ADV-SCS SRMS	OPT-SO NOS-ASCS SRMS
Third Party Risk Program Development	OPT-SOS ADV-SCS TRPD	OPT-SO NOS-ASCS TRPD
HIPAA and HITECH Assessment	OPT-SOS ADV-SCS HHA	OPT-SO NOS-ASCS HHA
PCI ASV Scanning	OPT-SOS ADV-SCS PASV	OPT-SO NOS-ASCS PASV
Custom Security Consulting Services	OPT-SOS ADV-SCS CSC	OPT-SO NOS-ASCS CSC
Security Segmentation Service	OPT-SOS ADV-SCS SSS	OPT-SO NOS-ASCS SSS
Enterprise Security Advisor	OPT-SOS ADV-SCS SAA	OPT-SO NOS-ASCS SAA