



## Service Description: Security Architecture Assessment Service

This document describes the Security Architecture Assessment (SAA) Service.

**Related Documents:** This document should be read in conjunction with the following documents also posted at [www.cisco.com/go/servicedescriptions/](http://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), Advanced Services Agreement (ASA), or equivalent services agreement executed between you and Cisco. In the event of a conflict between this Service Description and your MSA or equivalent services agreement, 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/](http://www.cisco.com/go/servicedescriptions/).

Cisco shall provide the Security Architecture Assessment 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") 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 between the parties and that, additionally, acknowledges and agrees to the terms contained therein.

### Service Summary

Security Architecture Assessment Services provide a comprehensive vendor-agnostic and industry best practices based assessment of the technical controls of the Customer's IT infrastructure using the Cisco Security Control Framework (Cisco SCF). The framework is consistent with international standards including the ISO 27000 series and NIST 800-53, as well as the most common regulatory and industry compliance standards for security. Cisco in conjunction with Customer's representatives shall scope the assessment based on the Quote and the Customer's environment. Cisco shall then collect information from Customer's representatives and network devices to assess the security architecture. Based on this assessment, Cisco shall provide a report of gaps in the

Customer's security architecture. Cisco shall also provide prioritized recommendations to mitigate the identified risks, including improvements to topology, protocols, device configurations, and security management tools.

The Security Architecture Assessment is composed of eight individual assessments that apply to different functional blocks in the IT infrastructure. The required Internal SAA provides the base assessment for all other assessments and can be conducted independently or in conjunction with any combination of the other assessments including: Perimeter, Unified Communications, Data Center, Wireless, Endpoint, Firewall Rules and Physical.

### Security Architecture Assessment (SAA) Service

#### Cisco Responsibilities

Under this Service, Cisco shall provide the Security Architecture Assessment Service during Standard Business Hours, unless stated otherwise. Cisco shall provide the following General Service provisions for any SAA specified in the Quote:

#### General Service Responsibilities

- 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 and any 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 Project 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 SAA hereunder. Customer may 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.

- Cisco Advanced Services Engineer shall conduct the SAA using the Cisco Security Control Framework. The Cisco Engineer shall perform the following tasks for any of the assessments unless specifically noted below:
  - **Scope and Collect:** Cisco Engineer shall conduct a one (1) day workshop at the Customer's site with the Customer's representatives to gather information related to the Customer's business environment and IT infrastructure. Specific activities performed during the scope and collect phase include:
    - Conduct discussions, interviews, and whiteboard sessions with the Customer's representatives to gather general information about Customer's:
      - Business and infrastructure architecture
      - Compliance requirements
      - Future business plans that affect the business environment or IT infrastructure
      - Security organization
      - Security concerns and previous incidents
    - Identify specific IT infrastructure assets to include in assessment
    - Conduct interviews; complete checklists; and collect detailed information about network topology, architecture and design documents; device configurations, and configuration templates
    - Refine collected information remotely through e-mail and phone conversations with Customer's representatives
  - **Assess:** Cisco Engineer shall assess the Customer's infrastructure architecture with respect to the Cisco Security Control Framework/Technical Control Set. Specific activities performed during the assess phase include:
    - Identify architectural techniques used to implement each control
    - Assess effectiveness of techniques
    - Evaluate how widely techniques are deployed
    - Score controls
  - **Report:** Cisco Engineer shall conduct a one (1) day session at the Customer's site to deliver the final report and executive presentation. Specific information included in the report and presentation include:
    - Identified gaps in controls based on lack of architectural support for the control or incomplete deployment of control
    - Evaluation of gaps relative to business objectives

- Remediation recommendations for the highest level risks

### Specific Service Responsibilities

Under this Service, Cisco shall perform the corresponding activities shown below for each individual assessment selected and specified in the Quote:

#### • **Internal Security Architecture Assessment**

Cisco shall assess the effectiveness of the Cisco Security Control Framework/Technical Control Set in the internal network infrastructure including WANs and LANs for core, campus and individual sites as specified in the Quote. The assessment also covers common security infrastructure controls that apply to many infrastructure domains such as access control, identity management, network management, intrusion detection and prevention, security event management and logging. Based on the scope of the assessment, specific information collected during the Internal SAA may include:

- Network architecture description
- Standards for network infrastructure
- Applications and services running over the network (VoIP, video streaming, terminal emulation, http, ftp, etc.)
- Key network assets, applications and services
- Physical and logical network topology diagrams, including the location of the devices included in assessment
- High-level architecture of data center, internal servers, user host connectivity and Internet connectivity
- Network Management System architecture

#### • **Perimeter Security Architecture Assessment**

Cisco shall assess the effectiveness of the Cisco Security Control Framework/Technical Control Set in the security infrastructure that protects the Customer's network perimeter including internet access, employee remote access, extranet, guest networks, and e-commerce sites as specified in the Quote. Based on the scope of the assessment, specific information collected during the Perimeter SAA may include:

- Network architecture description
- Standards for network infrastructure
- High-level architecture of network perimeter
- Services that traverse the perimeter network
- Key perimeter network assets, application and services
- Physical and logical perimeter network topology diagrams, including the location of the devices included in assessment
- Network Management System architecture

- **Unified Communications Security Architecture Assessment**

Cisco shall assess the effectiveness of the Cisco Security Control Framework/Technical Control Set in the security infrastructure that protects the Customer's Unified Communications system as specified in the Quote. The assessment covers call processing, endpoints, applications and the underlying network that carry the communications traffic. Based on the scope of the assessment, specific information collected during the Unified Communications SAA may include:

- Physical and logical network topology, architecture and design diagrams for the foundation network for voice and video traffic, including the location of the devices included in assessment
- Call Processing, Endpoint and UC application, topology, architecture and design documents
- Existing Cisco Unified Communications Manager and Unity audit documents, software risk assessments, and software versions

- **Data Center Security Architecture Assessment**

Cisco shall assess the effectiveness of the Cisco Security Control Framework/Technical Control Set in the security infrastructure that protects the key components of a Data Center including the storage network, server farm, services aggregation, core, distribution, access, and edge networks as specified in the Quote. This assessment takes virtualization into consideration, from a network and host perspective. Based on the scope of the assessment, specific information collected during the Data Center SAA may include:

- Physical and logical network topology, architecture and design diagrams for the Data Center routing and switching network, including the location of the devices included in the assessment
- Security appliance configurations and templates: firewall, intrusion detection and prevention, distributed denial of service, application firewall, web firewall
- Server virtualization architecture
- Application infrastructure and service offerings
- Storage area network topology and architecture

- **Wireless Security Architecture Assessment**

Cisco shall assess the effectiveness of the Cisco Security Control Framework/Technical Control Set in the security infrastructure that protects the Customer's wireless and associated network infrastructure, including local and guest controllers, access points, and WLAN clients as specified in the Quote. Based on the scope of the assessment, specific information collected during the Wireless SAA may include:

- Physical and logical network topology, architecture and design diagrams for the Wireless network controllers and access points, including the location of the devices included in the assessment.

- Access point and controller configurations and templates

- **Endpoint Security Architecture Assessment**

Cisco shall assess the effectiveness of the Cisco Security Control Framework/Technical Control Set in the security infrastructure that protects the hosts and endpoints not residing in the data center, including laptops, PCs, servers, and other devices connected to the network as specified in the Quote. Based on the scope of the assessment, specific information collected during the Endpoint SAA may include:

- Endpoint management and software deployment mechanisms
- Details of endpoint security software for anti-virus and anti-spyware
- Permitted end user applications and access
- IT support staff size and location
- Desktops and laptops: number; share policies; and standard and permitted applications
- Servers: domain structure, applications, external access

- **Firewall Rules Security Assessment**

Cisco shall assess the effectiveness of the Customer's firewalls by evaluating the firewall configuration, rule base, and deployment architecture against industry best practices and Customer business requirements as specified in the Quote. Based on the scope of the assessment, specific information collected during the Firewall Rules Assessment includes:

- Firewall Architecture Diagrams
- Firewall rules files and rule templates
- Details of protected assets and services provided across firewall

- **Physical Security Architecture Assessment**

Cisco shall assess the effectiveness of the Cisco Security Control Framework/Technical Control Set in the security infrastructure that protects a Customer from un-authorized physical access as specified in the Quote. Technologies that will be evaluated span the range from physical barriers and locks to electronic badge-readers, video surveillance, and associated facility monitoring systems. Based on the scope of the assessment, specific information collected during the Physical SAA may include:

- Standards and design documents related to physical security
  - Perimeter of facilities, including:
  - Entry control and identity verification
  - Material control
  - Communications

- Fire protection
- Building safety interfaces (sensors and alarms)
- HVAC (sensors and alarms)
- Environmental (power supply and generation, lighting, occupancy sensors and alarms)
- Infrastructure and Data Center physical security and access control
- Security management system

### **Customer Responsibilities**

#### **General Service Responsibilities**

Customer shall comply with the following obligations:

- Customer shall designate a person to whom all Cisco communications may be addressed and who has the authority to act on all aspects of the Service. Customer shall also designate a back up when the Customer contact is not available who has the authority to act on all aspects of the Services in the absence of the primary contact.
- In the event the Network composition is altered, after this Exhibit is in effect, Customer is responsible to notify Cisco in writing within ten (10) days of the change. Cisco may require modifications to the fee if the Network composition has increased beyond the original pricing quote for Services.
- Provide a high-level architectural drawing showing the type of Hardware, Software, and application solution configurations and where they are physically located (for example, geographical location or location within the Network).
- Provide a list of all of the existing security architecture components including but not limited to Hardware, Software and solution configurations; architecture descriptions.
- Provide security network expansion roadmap.
- Provide detailed definitions of the type of application (for example mobile traveler, corporate workforce) and features; detailed definition of Customer's implementation strategy.
- Provide copies of product configurations and templates.
- Ensure key Customer networking and operational personnel are available to participate in interview sessions as required.
- Unless otherwise agreed to by the parties, Customer shall respond within two (2) business days of Cisco's request for documentation or information needed for the Service.
- Provide proper security clearances and/or escorts as required to access the Customer's facility.
- Supply the workplace policies, conditions and environment in effect at 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.

#### **Specific Service Responsibilities**

- **Internal Security Architecture Assessment.** In addition to the General Responsibilities, Customer shall:

Provide access to the appropriate resources with knowledge and authority to provide Cisco with the following information:

- Standards for network infrastructure
  - Configuration templates
  - IOS versions
- Applications and services running over the network (VoIP, video streaming, terminal emulation, http, ftp, etc.)
- Key network assets, applications and services
- Physical and logical network topology diagrams, including the location of the devices included in assessment
  - Core, distribution and access layers
  - Firewalls
  - DMZs
  - IDS/IPS
- High-level architecture of data center, internal servers, user host connectivity and Internet connectivity
- Network architecture description
  - Resilience
  - Routing
  - NTP
- Network Management System architecture
  - Network management module
  - Management network
  - Management protocols
  - Management systems
  - Logging
  - Future network plans

- **Perimeter Security Architecture Assessment.** In addition to the General Responsibilities, Customer shall:

Provide access to the appropriate resources with knowledge and authority to provide Cisco with the following information:

- Standards for network infrastructure
  - Configuration templates
  - IOS versions
- High-level architecture of network perimeter
  - Internet access
  - Remote access
  - Extranet
  - DNS
  - E-commerce
- Services that traverse the perimeter network
  - http
  - ftp
  - email
- Key perimeter network assets, application and services
- Physical and logical perimeter network topology diagrams, including the location of the devices included in assessment
  - Internet gateway routers,
  - Firewalls
  - DMZ
  - Remote access devices
  - Switches and associated internal devices (first hop routers in the internal network)
  - IDS/IPS security devices
- Network architecture description
  - Resilience
  - Routing
  - NTP
- Network Management System architecture
  - Network management module
  - Management network
  - Management protocols
  - Management systems
  - Logging
  - Future network plans

- **Unified Communications Security Architecture Assessment.** In addition to the General Responsibilities, Customer shall:

Provide access to the appropriate resources with knowledge and authority to provide Cisco with the following information:

- Physical and logical network topology, architecture and design diagrams for the foundation network for voice and video traffic, including the location of the devices included in assessment
- Call Processing, Endpoint and UC application, topology, architecture and design documents
- CUCM, Unity audit documents, software risk assessments, software versions
- **Data Center Security Architecture Assessment.** In addition to the General Responsibilities, Customer shall:
 

Provide access to the appropriate resources with knowledge and authority to provide Cisco with the following information:

  - Physical and logical network topology, architecture and design diagrams for the Data Center routing and switching network, including the location of the devices included in the assessment
  - Security appliance configurations and templates: firewall, intrusion detection and prevention, distributed denial of service, application firewall, web firewall
  - Server virtualization architecture
  - Application infrastructure and service offerings
  - Storage area network topology and architecture
- **Wireless Security Architecture Assessment.** In addition to the General Responsibilities, Customer shall:
 

Provide access to the appropriate resources with knowledge and authority to provide Cisco with the following information:

  - Physical and logical network topology, architecture and design diagrams for the Wireless network controllers and access points, including the location of the devices included in the assessment.
  - Access point and controller configurations and templates
- **Endpoint Security Architecture Assessment.** In addition to the General Responsibilities, Customer shall:
 

Provide access to the appropriate resources with knowledge and authority to provide Cisco with the following information:

  - Endpoint management and software deployment mechanisms
  - Details of endpoint security software for antivirus and antispyware
  - Permitted end user applications and access

- IT support staff size and location
- Desktops and laptops: number; share policies; and standard and permitted applications
- Servers: domain structure, applications, external access

- **Firewall Rules Security Assessment.** In addition to the General Responsibilities, Customer shall:

Provide access to the appropriate resources with knowledge and authority to provide Cisco with the following information:

- Firewall rules files
- Firewall configurations and templates
- Firewall Architecture Diagrams
- Details of protected assets and services provided across firewall

- **Physical Security Architecture Assessment.** In addition to the General Responsibilities, Customer shall:

Provide access to the appropriate resources with knowledge and authority to provide Cisco with the following information:

- Standards and design documents related to physical security
  - Perimeter of facilities, including:
    - Barriers
    - Sensor and Sensor Alarms
    - Lighting
  - Entry control and identity verification
  - Material control
  - Communications
  - Fire protection
  - Building safety interfaces (sensors and alarms)
  - HVAC (sensors and alarms)
  - Environmental (power supply and generation, lighting, occupancy sensors and alarms)
  - Infrastructure and Data Center physical security and access control
  - Security management system