Service Description: Advanced Services – Fixed Price

Cisco Security Advisory Services: Commercial Security Program and Control Design Assessment

ASF-CORE-SECPRGM

This document describes the fixed price Cisco Security Advisory Service for Commercial Security Program and Control Design Assessment.

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. 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 for your own internal use, this document is incorporated into your Master Services Agreement, Advanced Services Agreement, or other services agreement covering the purchase of Advanced Services-based services with Cisco ("Master Agreement") If no such Master Agreement exists, then this Service Description will be governed by the terms and conditions set forth in the Terms & Conditions Agreement posted at www.cisco.com/go/legalterms. If you have purchased these Services directly from Cisco for resale purposes, this document is incorporated into your System Integrator Agreement or other services agreement covering the resale of Advanced Services ("Master Resale Agreement"). If the Master Resale Agreement does not contain the terms for the Purchase and Resale of Cisco Advanced Services or equivalent terms and conditions, then this Service Description will be governed by the terms and conditions of the Master Resale Agreement and those terms and conditions set forth in the SOW Resale Terms & Conditions Agreement posted at www.cisco.com/go/legalterms. For purposes of the SOW Resale Terms and Conditions this Service Description shall be deemed as a Statement of Work ("SOW"). In the event of a conflict between this Service Description and the Master Agreement or equivalent services exhibit or 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/.

Commercial Security Program and Control Design Assessment

Service Summary

Cisco will review the business requirements for, and assess the maturity of, the Customer's Security Program. This assessment provides recommendations to align security investments with the Customer's business strategy and mitigate risks based on control implementation that is not aligned to leading security practices.

Cisco will leverage onsite interviews and review of appropriate documentation to develop requirements and recommend target state maturity of Customer's security management program, operational processes, and technical control implementations. Cisco will also conduct a baseline review of the Customer's current security management program, operational processes, and technical controls to determine current maturity to identify gaps and recommend a security program improvement roadmap.

Location of Services

Service will be delivered on-site at one Customer location (up to 12 interviews with key business and security/IT leaders).

Travel will be limited to no more than one (1) visit by Cisco of up to five (5) days total on-site at a single Customer location.

Information Security Program Context

Cisco Responsibilities

- Establish Information Security Program Context;
  - Review documentation and conduct interviews to gain understanding of the Customer's security organization, business context, risk tolerance, regulatory compliance requirements, and expectations for data protection and information security.
  - Based on management input, recommend a target state maturity for Customer's information security program.

- Identify appropriate stakeholders for the interview phase of the assessment.

Customer Responsibilities

- 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 Cisco with access to appropriate building access and badges, workspace, meeting space, telephone and LAN access for team members.

Information Security Program Maturity Assessment

Cisco Responsibilities

- Conduct Information Security Program Maturity Assessment ;
  - Assess the maturity of the Customer's information security program within management and strategy, operations, and technology areas of analysis.
  - Review the organization and information security goals
  - Interview up to 12 stakeholders to understand information security strategies, policies, processes, and procedures;
    - Gain a high level understanding of the security architecture.
    - Review relevant security governance Processes.
    - Review Customer's stated implementation of security processes and controls.
  - Review documentation, including ;
    - Most recent information security risk Assessment.
    - Information security policies and standards
    - Standard configurations
    - Relevant operational security processes
  - Document current state security program maturity and recommend the appropriate level of maturity based upon management expectations and business context.
  - Develop a roadmap of security initiatives based on Customer priorities.
  - Provide Customer with the Information Security Maturity Assessment Report.
  - Provide Customer an Executive Summary Presentation, not to exceed one (1) hour.

Customer Responsibilities

- 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.
- Review with Cisco the completed Security Program Assessment Report.

General Customer Responsibilities

- Customer represents and warrants that they have sufficient authority and the rights necessary for Customer to provide and/or facilitate Cisco's access to information, data, networks, systems, and media in connection with these Services.
- For all Customer requests under this Service Description that Cisco possess, access, or analyze particular media, computers, computer networks, communications networks, or other systems and equipment, to the extent Customer provides or facilitates Cisco's access thereto, Customer represents, warrants and covenants that they have all necessary right, title, license, and authority to make such requests and grant such access, including all necessary permissions from third-party owners of licensed or shared resources.
- CUSTOMER IS RESPONSIBLE FOR OBTAINING ALL NECESSARY LICENSES, PERMISSIONS, AND CLEARANCES FOR CISCO TO ACCESS RESOURCES THAT ARE HOSTED, OWNED BY, OR SHARED WITH A THIRD-PARTY.
- Customer is responsible for provisioning of necessary test access, environments, VPN connections, user accounts, administrative access, or other required technical assets.
- All information (such as but not limited to: designs, topologies, requirements) provided by Customer is assumed to be up-to-date and valid for the Customer's current environment. Cisco Services are based upon information provided to Cisco by Customer at the time of the Services.
- Customer acknowledges that the completion of Services is dependent upon Customer meeting its responsibilities as indicated herein.
- Customer will identify Customer's personnel and define their roles in the participation of the Services. Such personnel may include but is not limited to: architecture design and planning engineers, and network engineers.
- Customer will ensure Customer's personnel are available to participate during the course of the Services to provide information and to participate in scheduled information gathering sessions, interviews, meetings and conference calls.
- Customer expressly understands and agrees that support services provided by Cisco comprise technical advice, assistance and guidance only.
- Customer expressly understands and agrees that the Services shall take place and complete within ninety (90) calendar days from issuing a Purchase Order to Cisco for the Services herein and any unused hours will expire.

Invoicing and Completion

Invoicing

Services will be invoiced upon completion of the Services.

Completion of Services

Cisco will provide written notification upon completion of the Services to Customer. The Customer shall within five (5) Business Days of receipt of such notification provide written acknowledgement of Cisco's completion of the Services. Customer's failure to acknowledge completion of the Services or to provide reasons for rejection of the Services within the five (5) Business Day period signifies Customer's acceptance of completion of the Services in accordance with this Service Description.

Assumptions and Exclusions

- Customer is solely responsible for determination and implementation of its network, design, business or other requirements and the implementation of any recommendations provided by Cisco. Cisco's recommendations are based upon Customer information provided to Cisco. Cisco shall not be liable for the accuracy or completeness of any Customer information contained in Cisco's recommendations.
- All documents will be provided in electronic form in the English language.
- Customer retains all responsibility for the security of Customer Technical Environment(s). Cisco shall have no responsibility for, or liability as a result of, any breach in security of Customer's Environment. Cisco cannot guarantee that Customer's security may or may not be vulnerable from any included, omitted or overlooked instances whether or not presented in the Services or Deliverables associated with this Service Description.
- Security assessment services will not definitively prove the absence of vulnerabilities.