CISCO BUSINESS CRITICAL SERVICES

ACCELERATION THEME

This document contains the detailed description of capabilities and Deliverables aligned to Cisco Business Critical Services Acceleration theme.

Note: This document must be read in conjunction with the Cisco Business Critical Services General Terms.

CISCO BUSINESS CRITICAL SERVICES GENERAL TERMS

https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco_Business_Critical_Services_General_Terms.pdf

Detailed descriptions of capabilities and Deliverables aligned to all Cisco Business Critical Services themes are located at:

CISCO BUSINESS CRITICAL SERVICES FOUNDATION THEME

https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco_Business_Critical_Services_Foundation_Theme.pdf

CISCO BUSINESS CRITICAL SERVICES ACCELERATION THEME

https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco_Business_Critical_Services_Acceleration_Theme.pdf

CISCO BUSINESS CRITICAL SERVICES TRANSFORMATION THEME

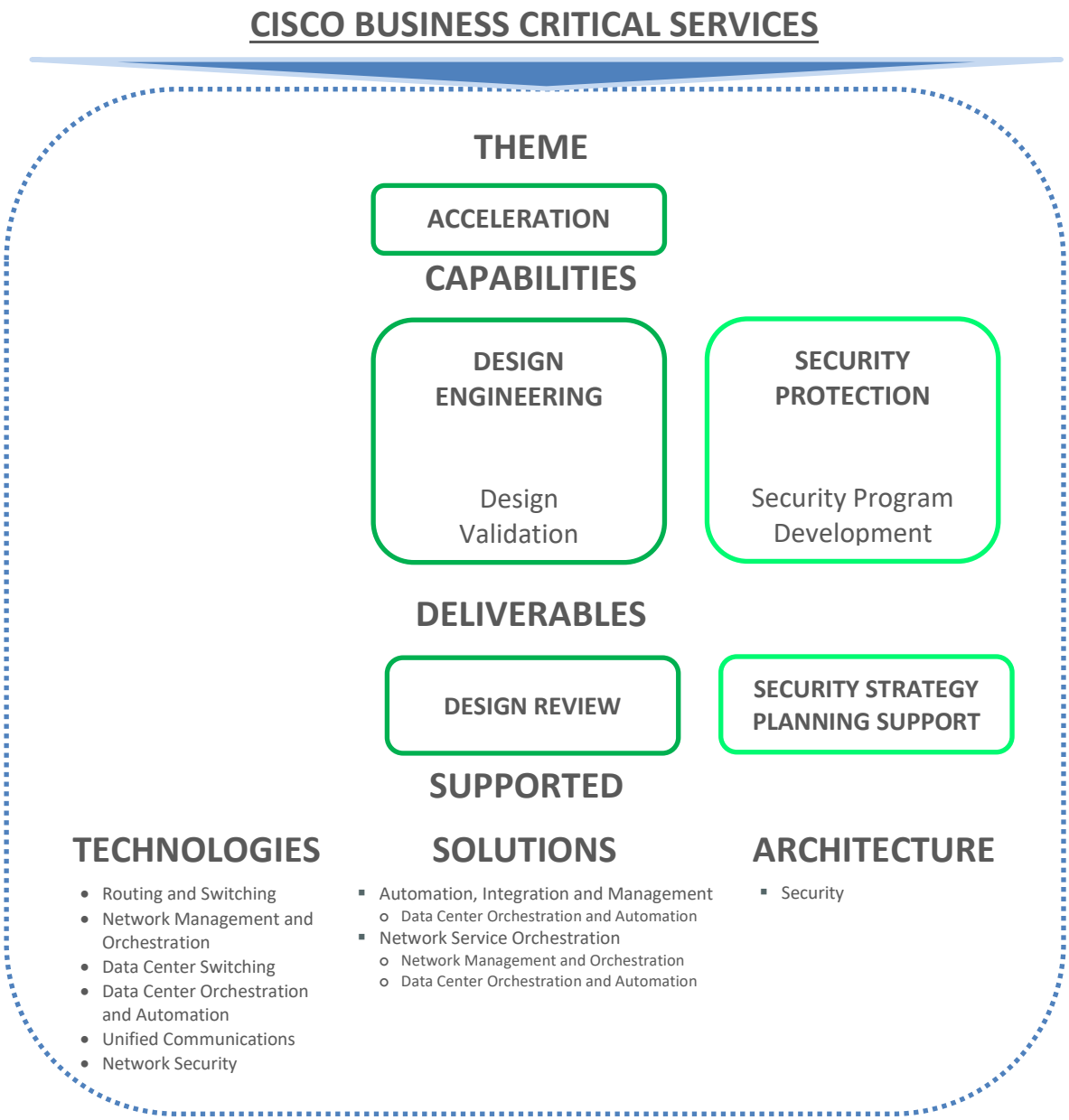
https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco_Business_Critical_Services_Transformation_Theme.pdf

TABLE OF CONTENTS

ACCELERATION THEME OVERVIEW

The **Acceleration theme** of Cisco Business Critical Services provides capabilities and Deliverables in support of design and validation, application insights, threat analytics, automation, Security programs, and hardening of Cisco infrastructure and application environment. Deliverables described in the Cisco Business Critical Services Acceleration theme are aligned by capabilities, and supported technologies, solutions or architectures.

Note: The diagram below is for illustrative purposes only.



ACCELERATION THEME CAPABILITIES AND DELIVERABLES

Acceleration capabilities and deliverables help Customers quickly scale and adapt to changing requirements, technologies, and increased pace of change within their infrastructure and applications.

1—DESIGN ENGINEERING

Design Engineering helps Customers apply design, validation, and feature engineering leading practices, insights and recommendations to help accelerate and expand their infrastructure and applications design.

SECTION NAVIGATION

Acceleration Theme – Design Engineering includes the following Service capabilities and Deliverables, each bookmarked for easier navigation:

1.1 – Design and Validation

Design and Validation focuses on providing recommendations and assistance with developing, enhancing, validating, and supporting applications, and infrastructure designs to achieve Customer business and solution engineering objectives.

1.1.1 – Design Review

Design Review provides assistance in verifying that Customer designs incorporate Cisco's best practices to achieve current and future business and technical functionality, resiliency, efficiency, and scaling requirements.

The review focuses on assessing Customer Solution and technical design requirements, performing a current-state capability and risk assessment, and providing design recommendations for achieving Customer objectives.

Technologies Supported

- Routing and Switching
- Optical Networking
- Wireless Networking
- Network Management and Orchestration
- Computing Systems
- Storage Area Networking
- Data Center Switching
- Network Security
- Cloud Security
- Security Policy and Access
- Advanced Threat
- Packet Core
- Mobility Policy and Access
- Next-Gen Cable Access
- SP Video Infrastructure
- Industrial Networking and Collaboration

Solutions Supported

- Software Defined WAN
  - Routing and Switching
  - Network Management and Orchestration
- Virtual Packet Core
  - Packet Core
- Self-Optimizing Network
  - Mobility Policy and Access
- SP Analytics and Assurance
  - Network Management and Orchestration

Cisco Responsibilities

- Analyze impact and risk of new requirements and changes (such as configurations and protocols) on existing design.
- Develop a future design deployment roadmap optimized for resiliency, availability, Security, and scalability.
- Verify that the recommended platforms, features, and functionality will meet Customer's communicated design objectives.
- Recommend and review changes to the design information, which may include:
  - Changes to high-level or low-level design.
  - Key risks and recommended contingencies in the proposed design changes.

- Logical and physical topology and architecture and, if applicable, topology diagram
- Provisioning policies.
- Configuration templates for Cisco devices.
- Cisco Software features and/or functionality.
- Hardware platform compatibility.
- Business / service continuity and disaster recovery.
- Operational efficiency improvements through new features, configuration Updates, and process improvements.

Note: Cisco is not responsible for developing design documents as part of this Deliverable, but will assist in answering design questions related to new feature implementation.

Deliverable

- Design Review Report

Customer Responsibilities

- Develop the complete design document for any new features or new application deployment.
- Revise and update the Customer Acceptance Test and Ongoing Support Plan for detailed design as recommended by Cisco.

Limitation

**Specific to Optical Networking*

- One (1) Design Review Report supports up to 20 devices.

1.1.1a – Design Review—Customer Care

The following call routing logic based Design Review responsibilities apply specifically to Customer Care in the areas outlined below:

- Script Design Review
- Precision Routing Design Review

Script Design Review

Technology Supported

- Customer Care

Cisco Responsibilities

- Discuss with the Customer the scripts to be reviewed.
- Review the pre-determined scripts identified by the Customer (up to 12 in total).
- Perform a script review of the select Customer-identified scripts and provide recommendations.
- Identify methodologies that conflict with leading practices and outline recommendations.
- Identify where scripts may be changed to improve efficiency in script administration.
- Review Customer scripts for consistency and alignment to repeatable standards.
- Present standardized script design strategies across applications and across enterprise.
- Collaborate and plan implementation strategy for recommended script modifications.

Deliverable

- Script Design Review Report

Customer Responsibilities

- Provide access to script library.
- Provide access to Customer or developer resource(s) to review the custom and third-party script components that interact with standard scripting.

Limitations

**Specific to Customer Care*

The following are not covered or a part of the Script Design Review for Customer Care:

- Script reviews and recommendations beyond the amount contracted.
- Cisco Unified Communications Manager (CUCM) configuration.
- Time-division multiplexing (TDM) automated call distribution (ACD) system configuration.
- Third-party applications, integrations, and script objects (e.g., custom Java).
- Voice recognition and text-to-speech scripts (except built-in).
- Custom-developed objects or code (e.g., custom Java code within Unified Customer Voice Portal Studio script).
- Reconciling of report data.
- Troubleshooting and escalation for Cisco Technical Assistance Center (TAC) issues related to scripting.

Precision Routing Design Review

Technology Supported

- Customer Care

Additional Information to be Collected

- Business process changes necessary to implement Precision Routing.
- Current business rules and proposed post-Precision Routing call routing.

Cisco Responsibilities

- Determine the following:
  - Which lines of business span multiple sites and require complex skill configuration and routing.
  - Reporting requirements and how existing reporting polices will need to change with the implementation of Precision Routing.
  - Current business rules and how they will change with the proposed Precision Routing call routing.
  - Call-flow diagrams to assess where Precision Routing fits and where it does not.
  - Skill-group configuration to determine who will benefit from Precision Routing.
  - Additional Documentation agreed upon during the kickoff meeting that details current business rules and proposed post-Precision Routing call routing.
- Present Precision Routing design strategies across lines of businesses, multiple sites, and enterprise.
- Present how queue treatment varies from one line of business to another.

- Collaborate with Customer to plan an implementation strategy.

Deliverable

- Precision Routing Design Review Report

Limitations

**Specific to Precision Routing Design Review for Customer Care*

The following are not covered or a part of the Precision Routing Design Review:

- Script reviews and recommendations beyond the amount contracted.
- CUCM configuration.
- TDM AC system configuration.
- Third-party applications, integrations, script objects (e.g., custom Java).
- Voice recognition and text-to-speech scripts (except built-in).
- Custom-developed objects or code (such as custom Java code within Unified Customer Voice Portal Studio script).
- Reconciling of report data.
- Troubleshooting and escalation for Cisco TAC issues related to scripting.

1.1.1b – Design Review—Data Center Orchestration and Automation

Design Review provides guidance and recommendations for Customer's current management automation tools infrastructure, such as orchestration, provisioning tools, and management portal, which are necessary to support a cloud computing architecture capable of offering cloud Infrastructure-as-a-Service (IaaS) or hybrid cloud infrastructure service.

Technology Supported

- Data Center Orchestration and Automation

Cisco Responsibilities

- Analyze the impact of new or additional integration requirements, and/or optimize the current deployment.
- Provide design assistance in aligning automation, integration, and management architecture evolution and Service model development.
- Review user interfaces, enabling the solution to be branded specifically to Customer's needs.

Deliverable

- Automation, Integration, and Management Design Assessment Report

1.1.1c – Design Review—Network Service Orchestration

This Design Review assists Customers to effectively design and implement Service Orchestration capabilities across their Cisco infrastructure.

Solution Supported

- Network Service Orchestration
  - Network Management and Orchestration

Cisco Responsibilities

- Analyze impact of new requirements on existing Service Orchestration.
- Provide design assistance in aligning Service Orchestration design with deployment architecture evolution and Service model development.

Deliverable

- Service Orchestration Design Report

1.1.2 – Ongoing Design Support

Ongoing Design Support provides guidance and recommendations in making incremental changes to Customer's designs. The review focuses on assessing Customer change requirements, performing a gap analysis based on current state design, and providing recommendations on implementation or modification of those designs based on published leading practices and industry standards.

Technologies Supported

- Routing and Switching
- Optical Networking
- Wireless Networking
- Network Management and Orchestration
- Computing Systems
- Storage Area Networking
- Data Center Switching
- Application Centric Infrastructure
- Data Center Orchestration and Automation
- Unified Communications
- Customer Care
- Video Collaboration
- Cloud Meetings and Messaging
- Network Security
- Cloud Security
- Security Policy and Access
- Advanced Threat
- Packet Core
- Mobility Policy and Access
- Next-Gen Cable Access
- SP Video Infrastructure
- Industrial Networking and Collaboration

Solutions Supported

- Network Service Orchestration
  - Network Management and Orchestration
  - Data Center Orchestration and Automation
- Virtual Packet Core
  - Computing Systems
- Software Defined WAN
  - Routing and Switching
  - Network Management and Orchestration
  - Packet Core

- Data Center Switching

Cisco Responsibilities

- Provide recommendations to implement Customer's design changes, including:
  - Known and potential risks involved.
  - Impact on Customer's current environment.
- Provide ongoing consultation for topics related to the above agreed-upon requirements that may impact the existing Customer design(s).

Note: Cisco is not responsible for developing design documents within this Service, but will assist in answering design questions related to new feature implementation.

Additional Responsibilities

**Specific to Unified Communications, Customer Care, Video Collaboration, Cloud Meetings & Messaging*

- Perform a review for each site model in multi-site deployments.
- Discuss Hardware and Software needed to accommodate capacity and growth requirements including issues related to end-of-sale or end-of-life components.
- Review Customer's step-by-step plan to address stated growth, providing recommendations to mitigate any potential issues.

**Specific to Application Centric Infrastructure*

- Provide support for design changes and enhancements to an existing Production Application Centric Infrastructure (ACI) fabric to meet new requirements related to scale and additional integration requirements, and/or to optimize the current architecture.
- Provide recommendations that may include, but are not limited to: low-level design changes in the Layer 2 or Layer 3 ACI fabric to support the new requirements.
- Provide summary of all design aspects, including routing, security, high availability, Layer 4 to Layer 7 (L4-L7) Services integration for standard, published, and supported device packages (Note: Excludes Hardware or Software configurations and support of third-party L4-L7 Service devices).

Deliverable

- Design Support Report

Limitations

**Specific to Data Center Orchestration and Automation*

- For Cisco CloudCenter (CCC) this Deliverable only supports the design of the following:
  - CloudCenter components
  - Applications and services built with the CloudCenter platform.

**Specific to Optical Networking*

  - One (1) Design Support Report supports up to 20 devices.

1.1.3 – DESIGN DEVELOPMENT

Design Development provides guidance and assistance in developing or improving Cisco infrastructure designs (High-Level or Low-Level).

Technologies Supported

- Routing and Switching
- Optical Networking
- Wireless Networking
- Network Security
- Cloud Security
- Advanced Threat
- Packet Core
- Mobility Policy and Access
- Security Policy and Access

Solution Supported

- Virtual Packet Core
  - Packet Core

Cisco Responsibilities

- Assist Customer to verify that the chosen platforms, features, and functionality will meet Customer's communicated design objectives.
- Assist Customer to create design document which may include the following:
  - Business, application, and technical objectives, and priorities.
  - High-Level Design or Low-Level Design requirements.
  - Design recommendations.
  - Key risks in the proposed design.
  - Logical and physical topology and architecture.
  - Configuration templates for Cisco infrastructure devices.
  - Software release recommendations based on design features and/or functionality.
  - Hardware and Software platform considerations.

Deliverable

- Design Document

Limitations

**Specific to Network Security; Cloud Security; Security Policy & Access; Advanced Threat*

- Cisco responsibilities 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.

**Specific to Optical Networking*

- Design Document support up to twenty (20) devices.

1.1.4 – Design Change Support

Design Change Support provides assistance in assessing the potential feasibility and impact of proposed changes to Customer designs.

The support focuses on evaluating Customer's design change requirements and risks, verifying Customer's change planning, implementation, support procedures, and providing Remote support to Customer staff during scheduled change windows.

Technologies Supported

- Routing and Switching
- Optical Networking
- Wireless Networking
- Computing Systems
- Storage Area Networking
- Data Center Switching
- Application Centric Infrastructure
- Packet Core
- Mobility Policy and Access
- Next-Gen Cable Access
- SP Video Infrastructure
- Industrial Networking and Collaboration

Solutions Supported

- SP Analytics and Assurance
  - Network Management and Orchestration
- Virtual Packet Core
  - Packet Core

Cisco Responsibilities

- Review Customer planning, implementation, and support processes related to proposed design change which may involve one or more of the following areas:
  - Change evaluation and planning priorities.
  - Change impact analysis on deployed architecture, designs, or configurations, application policies and functions.
  - Change implementation Methods of Procedures (MOP) based on Cisco best practices.
  - Potential risk mitigation priorities and required actions.
  - Change implementation support plan, resources, and roles.
  - Process to verify completion of change objectives.
  - Change back-out strategy related to scheduled design changes.
- Provide a Design Change Support Recommendations document that summarizes information gathered, analysis of findings, and recommendations (if Cisco determines necessary).
- Provide a designated Cisco Remote support contact to advise and respond to Customer requests during scheduled design change windows.
- Collaborate with Customer to verify systems readiness during design change windows at the request of the Customer.
- Work with Customer to make available, upon receipt of not less than twenty-one (21) days prior written request by Customer to Cisco, a designated support contact that can accept calls during Standard Business Hours, and consult with Customer on a 24-hours-a-day, 7-days-a-week standby basis.

Excluded Responsibilities

**Specific to Application Centric Infrastructure (ACI)*

- For ACI, Cisco will not provide a Design Change Support Recommendations Report.

Additional Responsibilities

**Specific to Network Security, Security Policy and Access, Cloud Security, Advanced Threat*

- Provide support for design changes to Customer plans (e.g. Network drawings, implementation plan, test plan and rollback plan), and configuration changes e.g. device configuration and cabling changes).

**Specific to MOP Document for Routing and Switching, Optical Networking, Wireless Networking, Computing Systems, Storage Area Networking, Data Center Switching, Packet Core*

- Provide recommended changes to Customer's implementation plan, method of procedure (MOP), and test plan based on information gathered from the Customer, analysis of proposed changes and Cisco best practices.
- Provide a MOP document for Cisco platform to Customer that may include the following in support of a design change:
  - Procedures performed prior to and following implementation of configuration and Software change.
  - Rollback procedures of scheduled configuration and or Software change.

Deliverables

- Design Change Support Recommendations Report
- MOP Document (specific to supported technologies)

Note: One MOP Document supports single proposed or planned design change of configuration and or Software update for a supported technology and Cisco platform.

Limitations

- Cisco is not responsible for testing any procedures in support of Customer's proposed or planned design changes.
- Cisco is not responsible for developing MOPs for non-Cisco platforms and technologies not specifically stated under Cisco Additional Responsibilities Specific to MOP Document.

**Specific to Network Security, Security Policy and Access, Cloud Security, Advanced Threat*

- 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.
- 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.
- 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.

**Specific to Optical Networking*

- One (1) Design Change Support supports up to twenty (20) devices.
- One (1) quantity of Design Change Support supports up to two (2) change support windows.

**Specific to MOP Document for the following technologies:*

Routing and Switching, Optical Networking, Wireless Networking, Computing Systems, Storage Area Networking, Data Center Switching, Packet Core

- Change impact analysis is not conducted using simulation tools.
- Cisco's verification of recommendations contained within the MOP document is limited to verification of configuration change, Software update and rollback procedures for up to one similar Cisco platform and operating system within Cisco's lab if Cisco deems it necessary.
- Cisco is not responsible for developing MOPs for any technologies not specifically stated under Cisco Additional Responsibilities Specific to MOP Document.
- MOP is not provided for migrating from one Cisco platform to another Cisco platform.

1.1.5 – Self-Optimized Network (SON) Scheduled Event / Venue Support

SON Scheduled Event / Venue Support provides proactive support to prepare for large-scale scheduled Customer events (games or conferences) that utilize Customer's Radio Access Network (RAN) resources. Cisco provides assistance to plan, implement, and support major SON application module configurations.

Solution Supported

- Self-Optimizing Network
  - Mobility Policy and Access

Additional Information to be Collected

- Business and technical requirements for Mass Event Handling (MEH) application module configuration.
- Scheduled Customer Event / Venue details

Cisco Responsibilities

- Assist Customer to configure MEH application modules to meet Customer event and venue networking requirements.
- Provide proactive support for Network freeze / rehome and any other major scheduled Radio Access Network (RAN) activities for SON.
- Review Customer RAN reports of anticipated network load or traffic.

Deliverable

- Consultative guidance and support only

1.1.6 – Test Strategy and Plan Review

Test Strategy and Plan Review provides assistance with evaluating Customer business and operational testing requirements and constraints, analyzing priority areas for review or improvement, providing a report with Cisco testing and lab strategy recommendations, and assisting Customer with test plan and analyzing results.

Technologies Supported

- Network Management and Orchestration
- Data Center Orchestration and Automation

Solutions Supported

- Network Service Orchestration
  - Network Management and Orchestration
  - Data Center Orchestration and Automation
- SP Analytics and Assurance
  - Network Management and Orchestration

Exclusion

**Specific to Data Center Orchestration and Automation*

- Cisco CloudCenter (CCC) is not supported.

Cisco Responsibilities

- Assist Customer to develop Test Plan or review / refine existing Test Plan, which defines the following scope:
  - Specific purpose for the entire Test Plan and for each test within the plan.
  - Required process or steps, dependencies, timeframe, and sequence of each test.
  - Required Cisco and third-party test Hardware devices and Software versions, including configurations and settings.
  - Measurable test outcomes so that a pass / fail result can be determined.
  - Responsibility matrix of Cisco and Customer responsibilities for executing the Test Plan.
- Assist Customer to execute the Test Plan, and document results.
- Analyze test results, and document Cisco's analysis of the results and recommendations in a Test Results Report.

Deliverables

- Testing and Lab Strategy Review Report
- Test Results Report

Customer Responsibilities

- Provide the physical test lab and equipment setup and configuration.
- Document and execute the Test Plan with Cisco's assistance.
- Provide Customer technical resources to run the specific test cases (scripts, workloads) on previously identified areas of the system as outlined in the Test Plan.
- Review and sign-off on the Test Results Report.
- Provide Remote Customer support as needed for pre-approved third party or Cisco competitor Products.
- Provide required third-party equipment or Cisco competitor equipment (including shipping to and from Cisco lab facility).

1.1.7 – Validation-Test Cycle and Review Standard

Validation-Test Cycle and Review Standard helps Customers plan and execute test cycle that is estimated to last between eight (8) and twelve (12) weeks. Testing may be performed at the Customer's Lab or Cisco Lab and will be indicated in the Quote.

Architectures Supported

- Core Networking
- Data Center and Cloud
- Collaboration
- Security
- SP Mobility
- SP Video

Cisco Responsibilities

- Perform analysis of requirements, such as Software strategy, platforms, topology, protocols, and configurations.
- Develop a Test Plan, or review / refine Customer's existing test plan.
- Execute the tests documented in the Test Plan, once agreed, and provide support that includes, but is not limited to:
  - Scheduling – Schedule facilities, equipment, and resources.
  - Test Setup – Set up the physical lab.
  - Test Automation – Develop and/or extend the automated test cases (or) scripts.
  - Test Execution – Execute the Test Plan.
  - Test Results Analysis – Document the results in a Test Report.

Note: Validation-Test Cycle and Review Standard is only available in certain geographic locations, and will be specified in the Quote for Services.

Deliverables

- Test Plan
- Test Report

1.1.8 – Validation-Test Automation

Validation-Test Automation helps Customer develop automation needs to validate and test the solution. Testing may be performed at the Customer's Lab or Cisco Lab and will be indicated in the Quote.

Architectures Supported

- Core Networking
- Data Center and Cloud
- Collaboration
- Security
- SP Mobility
- SP Video

Cisco Responsibilities

- Assess the availability of preferred test automation platforms within Customer's premise in case solution validation and test execution is performed within Customer's lab.
- Provide a Solution Validation and Automation Test Plan to Customer for review and approval.

- Develop test automation scripts based on the automation scope identified by Customer in Test Automation Plan.
- Provide access to the automation library so Customer has execution privileges for automation scripts.

Deliverables

- Solution Validation and Automation Test Plan
- Access to Test Automation Scripts

Customer Responsibilities

- Customer is responsible for providing testing and automation tools for testing performed in Customer's Lab.
- Collaborate with Cisco to identify required test cases and automation requirements.
- Identify any issues that may affect the setup and execution of the Test Plan.
- Adhere to the selected scheduling dates and times; if Customer must change test scheduling for any reason, then Change Management procedures would apply.

1.1.9 – Validation-Test Onsite Support

Validation-Test Onsite Support provides Customer with solution validation and test execution in the Customer's lab.

Architectures Supported

- Core Networking
- Data Center and Cloud
- Collaboration
- Security
- SP Mobility
- SP Video

Cisco Responsibilities

- Set up Customer-provided test and automation tools and methods of testing for solution infrastructure, configuration, integration, and aggregation points for the validation and test deployment, including protocols, security, and management considerations.
- Provide consulting and advising on test automation needs.
- Conduct tests based on the Test Plan.
- Provide Customer with On Site support for issues found during Customer testing phase.

Deliverables

- Test Plan
- Test Execution Report

Customer Responsibilities

- Customer is responsible for installation, rack / stack and cabling of Hardware, and for providing all Software, test, and automation tools required for conducting the tests.

1.1.10 – Validation-Test Persistent Lab Testing

Validation-Test Persistent Lab Testing helps Customers deploy a persistent lab in a Cisco lab facility that provides Solution Validation and Test Consulting Services which support and align with Customer's technology roadmaps.

Technologies Supported

- Core Networking
- Data Center and Cloud
- Collaboration
- Security
- SP Mobility
- SP Video

Cisco Responsibilities

- Develop solution validation and test plan strategy to align with technology roadmap.
- Execute test cycles that may include:
  - Review Customer Solution design, if applicable.
  - Review Customer test plans, if applicable.
  - Review and Update Customer test automation plans, if applicable.
  - Set up lab and test tools.
  - Execute Customer test plans.
  - Recommend modifications to the Customer design during test execution, if applicable.

Deliverables

- Test Plan
- Test Report

1.2 – Feature Engineering

Feature Engineering focuses on analyzing the benefits, risks, and methods of adopting advanced or upgraded application and infrastructure capabilities, while minimizing disruptions and risks to Customer's business by validating solution readiness.

1.2.1 – Advanced Feature Assessment

Advanced Feature Assessment assists Customer engineering staff to accelerate adopting advanced Cisco technology features that enhance Customer Solution functionality and resiliency. Cisco Engineers evaluate and plan solution requirements and dependencies for deploying advanced solution features in Customer's environment, while mitigating risks.

Technologies Supported

- Data Center Switching
- Tetration

Cisco Responsibilities

- Provide current design evaluation, implementation planning, and training for one (1) advanced feature that Customer will deploy.
- Perform system analysis on a selected domain of Customer's Cisco infrastructure for a specific advanced feature.
- Analyze infrastructure configurations, and align them with Customer's corporate policies and procedures as well as Cisco best practices.
- Review existing infrastructure design to determine the following:
  - Readiness and design requirements to deploy targeted advanced feature.
  - Ways to leverage targeted available infrastructure advanced feature in areas such as virtualization, resiliency, availability, and scalability.
- Work with Customer to develop a migration strategy to rollout the targeted infrastructure feature into Customer's existing environment.
- Conduct technology knowledge transfer session on targeted infrastructure advanced feature.

Deliverable

- Advanced Feature Analysis Report

Limitations

**Specific to Data Center Switching*

- Limited to current design evaluation, implementation planning, and knowledge transfer for one (1) advanced feature that the Customer will deploy

1.2.1a – Advanced Feature Assessment—Wireless Networking

Technology Supported

- Wireless Networking

Cisco Responsibilities

- Provide troubleshooting and system analysis Services that may include a detailed performance analysis of Customer's Wireless Network infrastructure using Cisco Wireless LAN (WLAN) Performance Analysis tools and techniques; the WLAN Performance and Security Analysis may include, among other activities:
  - Measuring the actual signal coverage of the wireless Network.
  - Identifying the overall level of interference and specific sources that may adversely impact Wireless Network performance.
  - Analyzing the Network utilization, Network RF signal tracking accuracy, and efficiency metrics of the Wireless Network.
  - Performing WLAN troubleshooting or packet capture and analysis for specific WLAN issues as needed.
  - Analyzing the Wireless Network Security design and configuration.

Deliverable

- Advanced Feature Analysis Report

Limitations

**Specific to Wireless Networking*

- An On Site Performance Analysis of the Customer's WLAN environment is limited to a maximum of ten (10) access points (AP) or 25,000 square feet.

1.2.2 – Migration Planning and Implementation Support

Migration Planning and Implementation Support assists Customer's engineering staff to accelerate updating Cisco Solutions while mitigating risks to infrastructure and Service stability.

Cisco Engineers assess Customer Solution migration environment or upgrade requirements, and verify solution design changes and dependencies and affected processes and Documentation. Cisco may also develop and verify qualified test cases in a lab environment, and provide Remote on-call support during scheduled Customer change windows, as specified in the Services quote.

Technologies Supported

- Network Management and Orchestration
- Data Center Orchestration and Automation
- Unified Communications
- Customer Care
- Video Collaboration
- Cloud Meetings and Messaging
- Hosted Collaboration Solution
- Packet Core
- Next-Gen Cable Access
- SP Video Infrastructure

Solutions Supported

- Network Service Orchestration
  - Network Management and Orchestration
  - Data Center Orchestration and Automation
- Virtual Packet Core
  - Packet Core

Exclusion

**Specific to Data Center Orchestration and Automation*

- Cisco CloudCenter (CCC) is not supported.

Additional Information to be Collected

- Application or solution dependency map, application owners, and system administrators.

Cisco Responsibilities

- Discover and analyze Customer environment (inventory, configurations and versions, traffic patterns) with Cisco tools.
- Determine potential, risks, or integration issues, and provide Cisco best practices around solution implementation and risk mitigation.
- Perform limited / qualified verification work in a Cisco lab to validate questions and recommendations.
- Develop qualified and agreed-upon remediation changes, and test in a Cisco lab to verify.

- Assist Customer with assessing and providing recommendations to Documentation change-control processes.
- Provide consultative support and guidance to Customer to understand required changes for remediation; Cisco will not perform any changes or modifications to the Customer environment.

Additional Responsibilities

**Specific to Network Management and Orchestration, Data Center Orchestration and Automation*

- Review the requisite list of high-level events, phased changes, and activities to introduce new Service Orchestration Solutions.
- Review Method of Procedure (MOP) Documentation for pre- and post-cutover connectivity and testing.
- Review master configuration templates for representative device or site types.
- Review solution test procedures for the ready-for-use (RFU) solution testing.

**Specific to Unified Communications, Customer Care, Video Collaboration, Cloud Meetings and Messaging, Hosted Collaboration Solution*

- Provide solution migration or implementation recommendations, including, but not limited to:
  - Step-by-step written procedures for Hardware and Software migration or implementation that are customized based upon Customer requirements.
  - Estimated level of effort associated with migration or implementation tasks.
  - Recommendations for Change Management procedures.
  - Documentation of Software and Hardware level for all dependent solution components.
  - Assistance to Customer in drafting or reviewing a test plan(s) to validate acceptance of migration or implementation.
  - Assistance to Customer in drafting or reviewing a migration or implementation contingency plan(s).

Deliverable

- Migration Planning and Implementation Recommendation Report

1.2.3 – VALIDATION-TEST STAGING

Validation-Test Staging helps Customer stage the solution in a Cisco Lab to plan and execute validation test cycles.

Architectures Supported

- Core Networking
- Data Center and Cloud
- Collaboration
- Security
- SP Mobility
- SP Video

Cisco Responsibilities

- Generate a proposed Test Plan, testing acceptance criteria, and staging timeline.
- Receive Customer's equipment, once agreed, and configure it.
- Execute the tests documented in the Test Plan, and report findings to the Customer.

- Notify Customer to arrange for the shipment of Customer equipment back to the Customer, following Cisco's notification to Customer of completion of testing.

Deliverables

- Test Plan
- Test Report

Customer Responsibilities

- It is the Customer's responsibility to pay for the shipping costs to Cisco's location and from Cisco's location to Customer's location.
- The Customer retains title and risk of loss while the staged equipment is at Cisco's location / lab for the testing / validation.

2—APPLICATION SUPPORT

Application Support provides assistance with analyzing the benefits, risks, and methods of integrating and supporting advanced or upgraded application and infrastructure capabilities, while minimizing disruptions and risks to Customer business.

SECTION NAVIGATION

Acceleration Theme – Application Support includes the following Service capabilities, each bookmarked for easier navigation:

2.1 – Custom Application Support

Custom Application Support focuses on assisting Customer to plan, configure, and support custom applications and automated processes.

2.1.1 – SITE AND SYSTEMS ADMINISTRATION SUPPORT

Site and Systems Administration Support is designed for Customer's site administrators responsible for the configuration, administration, and maintenance of the Cloud Management Platform, Tetration Analytics Solution, IT Workflow Automation, and/or Orchestration systems implementation.

Technologies Supported

- Network Management and Orchestration
- Data Center Orchestration and Automation
- Tetration

Solutions Supported

- Network Service Orchestration
  - Network Management and Orchestration
  - Data Center Orchestration and Automation
- Software Defined WAN
  - Network Management and Orchestration
- SP Analytics and Assurance
  - Network Management and Orchestration

Exclusion

**Specific to Data Center Orchestration and Automation*

- Cisco CloudCenter (CCC) is not supported.

Cisco Responsibilities

- Provide Remote support to Customer for the following activities that are generally performed:
  - Monitor environment(s):
    - Perform daily system health checks (log files, archive, and response times).
    - Provide proactive notification of errors, degradation, and other suspicious or unusual activity to appropriate contacts.
    - Monitor server utilization, memory, CPU, local storage, and throughput metrics.
    - Create weekly service level reports.
  - Maintain environment(s):
    - Apply hot fixes and upgrades.
    - Develop and maintain daily / weekly / monthly maintenance plans and processes.
    - Perform system restarts as required.
    - Work with Hardware operations for physical server maintenance as scheduled.
    - Maintain Security scheme and permissions.
    - Inspect settings and Software versions.
    - Check for consistency across environments.
    - Manage deployment-related issues (migration of objects from development to test to Production).
- Develop and document operational and system management processes (deployment models, user management, access controls).

**Specific to Tetration*

- Create up to two (2) Tetration Analytics Dashboards leveraging Tetration Analytics data with no more than four (4) tiles per dashboard.

Deliverable

- Operational and System Management Process Document

2.1.2 – SON Neighbor Discovery Support

SON Neighbor Discovery Support provides proactive configuration of new Customer Cell Site Neighbors. Cisco assists Customer to analyze, fine-tune, and support SON module configurations.

Solution Supported

- Self-Optimizing Network
  - Mobility Policy and Access

Additional Information to be Collected

- SON configuration requirements

Cisco Responsibilities

- Analyze Customer SON (Business Intelligence [BI]) traffic reports.
- Assist Customer to configure SON Automatic Neighbor Relations (ANR) module policy parameters.

- Assist Customer to configure Automatic Parameter Optimization (APO) module.
- Keep track of the RAN activities related to new Network elements.

Deliverable

- Consultative guidance and support only

2.1.3 – CUSTOMIZED BUSINESS CRITICAL INSIGHTS (BCI)

Customized BCI provides Customer the ability to specify use case(s) that can generate actionable insights for a Customer identified problem.

Use case(s) may include the following customized features supported by the Cisco Cloud Hosted Analytics and Insights Portal:

- **Visual Enhancements** such as but not limited to:
  - Dashboard modifications related to cosmetic, visual or time series change to existing feature for Platform Insights, Type 2 or Software Lifecycle Management, Type 2 Deliverables.
- **Portal Feature Development** such as but not limited to:
  - Customized feature(s) created using data collection supported by Cisco Data Collection Tools.
  - New correlation between data sets collected by Cisco Data Collection Tools.

Technology Supported

- Routing and Switching
- Wireless Networking
- Computing Systems
- Storage Area Networking
- Data Center Switching
- Network Security
- Security Policy and Access

Dependency

- Customer must have at least one (1) of the following Deliverables supported by Cisco Cloud Hosted Analytics and Insights Portal:
  - Platform Insights, Type 2
  - Software Lifecycle Management, Type 2
- Prior to the purchase of Customized BCI Deliverable, Customer and Cisco must complete a Use Case Discovery Template which includes the following information:
  - Customer identified problem and use case requirements.
  - Customer intended purpose and need for the use case.
  - Customer intended end user(s) for the personalized feature(s).
  - Number of personalized features and technologies.
  - Milestones and timelines for enabling personalized feature(s) within Cisco Insights and Analytics Portal.
- Customized BCI Deliverable must be renewed to continue delivery of customized features enabled within Cisco Cloud Hosted Analytics and Insights Portal following completion of Customer contract period.

Limitation

- This Deliverable only supports data collected using Cisco Data Collection Tools.

Additional Information to be Collected

- Completed Use Case Discovery Template

Cisco Responsibilities

Feature Commit Phase

- Build a conceptual representation of Customer use case using desktop software applications or Cisco lab environment to validate Customer requirements.
- Feature Commit Phase will be completed within two (2) months following project kickoff by Cisco Project Manager.

Feature Development and Testing Phase

- Develop and test use case within Cisco's lab environment.
- Gather Customer feedback from a maximum of up two (2) feature demonstration sessions within a two week time frame. Based on Customer feedback incorporate modifications agreed to by Cisco and within the scope of Customer validated requirements.
- Feature Development and Testing Phase will be completed within four (4) months after completion of the Feature Commit Phase.

Feature Activation Phase

- Provide one (1) session up two (2) hours to conduct feature walk through with Customer designated personnel.
- Feature Activation in Cisco Cloud Hosted Analytics and Insights Portal will be completed within one (1) month after completion of the Feature Development and Testing Phase.

Deliverable

- Customized BCI Feature

Note: The completed Use Case Discovery Template will specify the number of customized features and technologies in the quote.

2.2 – Custom Integration Support

Custom Integration Support focuses on assisting Customers to accelerate integrating custom applications and workflows using scripts and APIs.

2.2.1 – Management Solution Integration Support

Management Solution Integration Support assists Customer's engineering staff to accelerate adopting and integrating Cisco Management and Orchestration Software platforms or Third Party platforms with Customer workflow applications.

Cisco Engineers evaluate current and future state application workflow automation requirements, validate feature integration design changes, and resolve Customer questions and issues with standard published APIs.

Technologies Supported

- Network Management and Orchestration
- Data Center Orchestration and Automation
- Packet Core

Solutions Supported

- Network Service Orchestration
  - Network Management and Orchestration
  - Data Center Orchestration and Automation
- Software Defined WAN
  - Network Management and Orchestration
- SP Analytics and Assurance
  - Network Management and Orchestration

Note: Cisco Business Critical Services General Terms - General Cisco Responsibilities - Limitations contains the Cisco Platforms supported. Support for Third Party platforms will be specified in the Quote.

Additional Information to be Collected

- Customer Management and Orchestration design, objectives, requirements and priorities for application workflow automation, application integration, including standard Cisco APIs planned and implemented.

Cisco Responsibilities

- Diagnose Customer issues with the use or operation of the standard Cisco Management and Orchestration APIs.
- Advise Customer staff on standard Cisco API functional capabilities and usage within the context of overall Management and Orchestration workflow automation.
- Review and validate Customer application integration designs effectively utilize standard Cisco APIs.

Deliverable

- Consultative guidance and support only

Limitations

**Specific to Network Management and Orchestration, Data Center Orchestration and Automation, Network Service Orchestration, Software Defined WAN, SP Analytics and Assurance*

- The following are out of scope:
  - Design, development, deployment, and support of Customer workflow applications.
  - Testing of Customer workflow applications.
  - Assistance / support for non-Cisco Software APIs.

2.2.2 API Support for Customer Platform Integration

API Support for Customer Platform Integration provides Customer use of standard published APIs.

2.2.2a – ACI API Integration Support

ACI Application Programming Interfaces (API) Integration Support provides support for standard published API integration with VCenter and Cisco-approved and Cisco-supported L4-7 device packages.

Technology Supported

- Application Centric Infrastructure

Additional Information to be Collected

- API integration design and configuration.

Cisco Responsibilities

- Assist in deployment, and provide support for Customer integration work based on standard published API integration with VMware vCenter Server and Cisco-approved L4-L7 device packages.

Deliverable

- Consultative guidance and support only

Customer Responsibilities

- Complete Ongoing Design Support work item, which is a prerequisite for this work item.
- Work with ecosystem vendors for Service specific designs and configuration.

2.2.2b Business Critical Insights (BCI) API Library

BCI API Library provides Cisco-processed data in a machine consumable format via standard outbound APIs.

The following processed data features are supported via BCI API Library:

Processed Data - Platform Insights, Type 2 Portal Features

Base Membership Access to BCI API Library includes the following:

- Type 2 Standard Portal Feature: Hardware Lifecycle Milestones
- Type 2 Standard Portal Feature: Field Notices (if applicable)

Premium Membership Access to BCI API Library includes the following:

- Type 2 Standard Portal Feature: Configuration Best Practices
- Type 2 Optional Portal Feature: Policy Configuration Conformance
- Type 2 Optional Portal Feature: Third Party Feature Support

For a detailed description of the Platform Insights Type 2 Portal Features refer to the Cisco Business Critical Services Foundation theme document:

Processed Data - Software Lifecycle Management, Type 2 Portal Features

Base Membership Access to BCI API Library includes the following:

- Type 2 Standard Portal Feature: Software Lifecycle Milestones

Premium Membership Access to BCI API Library includes the following:

- Type 2 Standard Portal Feature: Software Track Conformance
- Type 2 Standard Portal Feature: PSIRT Analysis and Recommendation

For a detailed description of the Software Lifecycle Management Type 2 Portal Features refer to the Cisco Business Critical Services Foundation theme document:

Technologies Supported

- Routing and Switching
- Wireless Networking
- Computing Systems
- Storage Area Networking
- Data Center Switching
- Network Security
- Security Policy and Access

Dependencies

- Customer must have purchased the following Business Critical Insights Portal Features to access the corresponding processed data from the BCI API Library:
  - Platform Insights, Type 2
  - Software Lifecycle Management, Type 2
- BCI API Library uses an Entitlement Framework (EF) for onboarding Customer accounts and setting up role-based access control and privileges.
- A Cisco Connection Online (CCO) ID is required to access BCI API Library.

Limitations

- Processed data is updated weekly.
- BCI API Library does not provide historical, trending data and insights.
- APIs are Representational State Transfer (RESTful) protocol and data is returned Java Script Object Notation (JSON) format only.

Cisco Responsibilities

- Onboard Customer accounts and setup role-based access control and privileges.
- Provide API reference guide and access to Customer's processed data via Business Critical Insights API Library.

Customer Responsibilities

- Customer may not transmit any viruses, or other computer programs that may damage, detrimentally interfere with, surreptitiously intercept, or expropriate any system or data Cisco has granted access to.
- Customer may not attempt to reverse engineer or otherwise derive source code, trade secrets, or know-how of the BCI API Library.

- Customer may not use the BCI API Library to replicate or compete with core products or Services offered by Cisco.
- Customer may not use BCI API Library in a manner that accesses or uses any information beyond what Cisco allows under the terms of this Service; that changes the Cisco Service; that breaks or circumvents any of Cisco's technical, administrative, process or security measures; that disrupts or degrades the performance of the Service or the API Library; or that tests the vulnerability of Cisco's systems or networks.
- Customer will not attempt to exceed or circumvent limitations on access, calls and use of BCI API Library, or otherwise use the BCI API Library in a manner that exceeds reasonable request volume, constitutes excessive or abusive usage, or otherwise fails to comply with the terms of this Service.
- Customer may implement its own capability to monitor or track the success of requests to BCI API Library.
- Customer shall regularly monitor the quality of processed data accessed via BCI API Library and notify Cisco Services Project Manager of discrepancies.

Deliverable

- Access to BCI API Library.

Note: The BCI API Library Deliverable provides access to processed data for the supported Business Critical Insights features and technologies purchased in the quote.

3—SECURITY PROTECTION

Security Protection provides proactive Security strategies, planning, implementation guidance, training, simulations, and assists Customer with issue resolution.

SECTION NAVIGATION

Acceleration Theme – Security Protection includes the following Service capabilities and Deliverables, each bookmarked for easier navigation:

3.1 – Security Assessments

Security Assessments focus on uncovering technical vulnerabilities within IT systems and supporting infrastructure.

3.1.1 – PHYSICAL SECURITY ASSESSMENT

Physical Security Assessment performs testing of a Customer facility, attempting to exploit weaknesses in physical security controls to provide an opportunity to measure the effectiveness of physical security defenses and improve training efforts related to security awareness. The primary objective of the test is to gain access to valuable material and secure areas. The Physical Security Assessment will be conducted On Site at single low-security Customer facility that does not have high-Security defenses, such as mantraps, biometrics, or armed guards.

Architecture Supported

- Security

Cisco Responsibilities

- **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 identity and provisional purpose for being on site.
    - Attempt to gain physical access to defined facilities or areas (e.g., tailgating).
    - 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 Trojaned devices.
    - Place Trojaned 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.

Deliverable

- Physical Security Assessment Report

Customer Responsibilities

- Provide addresses and directions to reach and identify the physical location to be tested.
- 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 letter.
  - Identify any equipment or material authorized to be taken off the premises in the 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.

3.1.2 – Network Penetration Assessment

Network Penetration Assessment performs external or internal testing of a single Customer Network to identify high-risk and exploitable vulnerabilities, and to provide an opportunity to measure the effectiveness of security investments against a simulated threat. The primary objective of the test is to gain access to valuable Customer systems and data.

Architecture Supported

- Security

Cisco Responsibilities

- Perform intelligence gathering as follows:
  - Perform perimeter scans of protocols, Services, operating systems (OS), 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, XSS, 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, such as personally identifiable information (PII) and credit card numbers.
  - Attempt to pivot attacks to additional targets.
  - Attempt to exfiltrate data, as approved by the Customer.
- Provide the following reporting activities:
  - Eliminate false positives, where possible.
  - Investigate potential business impact.
  - Investigate and develop remediation strategies.

Deliverable

- Network Penetration Test Document

Limitations:

- Up to 256 external IP addresses or 400 internal IP addresses will be tested.

3.1.3 – Wireless Security Assessment

Wireless Security Assessment evaluates the deployment of the Customer's wireless environment for vulnerabilities at a Customer building. Security weaknesses may be demonstrated by exploiting the discovered weaknesses after Customer approval is provided.

Architecture Supported

- Security

Additional Information to be Collected

- Number of corporate 802.11 a / b / g / n / ac wireless APs, SSID, configuration state of SSID broadcasting, type of authentication, and encryption.

Cisco Responsibilities

- 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.
  - AP configuration.
  - Authentication and encryption.
- Identify and validate vulnerabilities.
- Rank vulnerabilities based on associated risk.

Deliverable

- Wireless Security Assessment Report

Customer Responsibilities

- Provide Cisco with authorization to exploit identified vulnerabilities, when required.

Limitations

- Cisco will conduct a Wireless Security Assessment of a single location.
- Cisco will enumerate up to five (5) unique, SSID-identified Wireless Networks, and evaluate the deployment of the wireless environment for vulnerabilities.

3.1.4 – Application Penetration Assessment

Application Penetration Assessment performs testing to identify application-layer vulnerabilities in a Customer-developed medium-sized application; however, the testing may discover vulnerabilities in the application's immediate dependencies. 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.

Architecture Supported

- Security

Additional Information to be Collected

- Application documentation, diagrams and access information (e.g. domain names, URLs, IP addresses).
- Details to fully execute the Application (e.g., example code, API documentation).
- User accounts for each role to be tested.
- Application source code for applications being assessed.
- Debug and production builds of target Software.

Cisco Responsibilities

- 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 that includes a range of techniques intended to identify security vulnerabilities in the most expedient manner possible, applying 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.
  - 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: Performing of activities to research vulnerabilities, eliminate false positives, and investigate the extent of the findings.

Deliverable

- Application Penetration Assessment Report

Customer Responsibilities

- 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.
- Identify any specifically targeted modules and their size (if applicable).
- Provide access to testing and Production environments (when applicable).
- Cover all costs associated with increased resource utilization on third-party systems (such as cloud providers) required by the testing.
- Notify and obtain testing authorization from any interested third parties.

Limitations

- Cisco will perform an Application Penetration Assessment of a single application for a single platform.
- 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.

3.1.5 – RED TEAM

Red Team performs testing to gain access to valuable Customer 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.

Architecture Supported

- Security

Cisco Responsibilities

- Perform intelligence gathering as follows:
  - Electronic asset information gathering, or 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 and sub-domains.
    - Identification of subsidiaries.
    - Performing of perimeter scans of live Services.
    - Identification of used OS, and other technologies.
    - Identification of Security defenses to be circumvented.
    - Identification of technologies in use.
    - Constructing a view of the attack surface.
  - Personnel information gathering as follows:
    - 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:
    - Perform 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, XSS, 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.
  - Perform 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., PII, credit card numbers).

Deliverable

- Red Team Analysis Report

Limitations

- The engagement will be restricted to remote attack vectors, such as direct attacks against Customer computers and users exposed on the Internet.

3.1.6 – Social Engineering Assessment

Social engineering Assessment identifies individual Customer staff requiring additional Security awareness training or obtains generalized Security awareness training success metrics that do not identify individuals (i.e., anonymized results). The testing may use text- or voice-based communication mechanisms such as email, 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.

Architecture Supported

- Security

Additional Information to be Collected

- Text-Based Social Engineering:
  - Provide a listing of target names and email addresses.
  - List targets that reported the social engineering attempts, when required.
- For Voice-Based Social Engineering:
  - Provide a listing of target names and phone numbers.
  - List targets that reported the social engineering attempts, when required.

Cisco Responsibilities

- Perform Text-Based Social Engineering:
  - Provide Customer with the source IP addresses of the email server(s) used to execute the campaign.
  - Identify highly exposed users using 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 websites.
    - 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 websites.
    - Attachments and files containing pseudo-malware.

    - Links to websites that mimic legitimate corporate websites designed to harvest credentials.
    - Links to web forms requesting the user submit sensitive data.
    - Impersonated identities of trusted individuals.
  - Monitor and record user responses
- Perform Voice-Based Social Engineering:
  - Identify highly exposed phone numbers or voice endpoints using OSINT methods.
  - Attempt to impersonate Customer-trusted identities, which may include Customer's customers, employees, and vendors.
  - Attempt to solicit up to twenty (20) individuals to provide sensitive information such as:
    - Access credentials.
    - Confidential information.
    - Financial data.
    - PII 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.

Deliverable

- Social Engineering Report

Customer Responsibilities

- For Text-Based Social Engineering:
  - Approve social engineering scenarios, when required.
  - Configure email servers, gateways, and filters to accept mails from the Cisco testing email server irrespective of transmission rate or content.
  - Ensure that individuals who should not receive phishing emails are clearly identified.
- For Voice-Based Social Engineering:
  - Approve social engineering scenarios, when required.
  - Ensure that individuals who should not receive phone calls are clearly identified.

Limitations

- For Text-Based Social Engineering:
  - Up to five-hundred (500) Customer-supplied email addresses, or thirty (30) Cisco-discovered but Customer-authorized email addresses, will be subject to phishing attacks.
  - Up to four (4) phishing campaigns will be conducted.
- For Voice-Based Social Engineering, Cisco will attempt to contact up to fifteen (15) employees.

3.2 – Security Program Development

Security Program Development focuses on assisting Customers to develop a suite of strategies, knowledge, organizational capabilities and processes, and measurements that help Customers achieve their business and Security objectives.

3.2.1 – Security Strategy Planning Support

Security Strategy Planning Support provides 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. Topics covered may include, but are not limited to, the following: Security Technologies and Architecture, Cloud, Cisco TrustSec® and Identity, Security Program, Security Governance Risk and Compliance, Automation and Control System Security, Mobile Security, Teleworking, Management, Data Center, and Collaboration Security.

Architecture Supported

- Security

Cisco Responsibilities

- Brief Customer on the Service and Service options.
- Conduct a Customer Pre-Planning Workshop.
- Conduct Customer Planning Workshop.
- Capture synopsis and recommendations from workshop.
- Perform a post-workshop analysis.
- Conduct post-workshop follow-up meeting.
- Capture synopsis and final recommendations following the post-workshop meeting.

Deliverable

- Work Summary Review

Limitations

- Workshop duration is up to three (3) days.
- 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, off-site, or Cisco TelePresence® workshop.
  - Up to three (3) follow-up meetings or one (1) full-day post-workshop meeting.
  - Up to four (4) concurrent Cisco participants.

3.2.2 – Information Security Risk Assessment and Program Development

Architecture Supported

- Security

Additional Information to be Collected

- IT risk organizational structure, team count, and field-of-view.
- Critical business processes, IT processes and their known application dependencies.
- Entity-level risk controls and governance processes.
- Stakeholder expectations, success factors for IT risk, perception, issues, or concerns of current process.
- Cultural factors that influence IT risk.

3.2.2a – Information Security Risk Assessment

Information Security Risk Assessment identifies, assesses, and recommends 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's understanding of risk tolerance gained through executive interviews, Cisco will develop a custom Information Security Risk Profile and Remediation Roadmap.

Cisco Responsibilities

- Customize the Risk Assessment based on the business context information collected.
- Formalize and agree on information security risk tolerance and business-relevant risk-rating criteria.
- Perform a strategic analysis of key strategic trends, taking into account:
  - Business strategies, Customer expectations, and relevant industry trends identified by stakeholders.
  - Relevant technology strategies.
  - Regulatory and legal trends.
  - Relevant information security and external threat trends.
- Review current IT risk process:
  - 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.
  - Review IT risk assessment reporting.
  - Investigate actionable outcomes and/organizational responses to IT risk assessment findings.
- Review and attempt to identify information security risks within Customer's business processes and IT architecture, infrastructure, and operational processes that support critical IT assets, which includes identifying potential risks and examining current controls via the following activities:

- Facilitate group Risk Assessment Workshop(s) with a subset of stakeholders to surface and assess risks based on informal institutional knowledge.
- Review available risk sources, such as Problem and Incident Management reports and IT performance metrics.
- Perform analysis of areas that may include, where relevant:
    - Information Security Governance and Oversight.
    - Information Security Policies, Standards, and Procedures.
    - Information Classification and Handling.
    - Compliance Processes.
    - Risk Assessment and Management.
    - Enterprise Security Architecture.
    - Security Metrics, Measurement, and Performance Management
    - Awareness and Education.
    - Vulnerability, Patch, Change, and Asset Management.
    - Security Monitoring and Instrumentation.
    - Incident Management.
    - Software Acquisition, Development, and Maintenance.
    - System Resiliency and Disaster Recovery.
    - Third-Party Risk Management.
    - Identity and Access Management.
    - Human Resources Security.
    - Physical and Environmental Security.
    - Network Security.
    - System Security.
    - Data Security and Encryption.
    - Mobile Devices and Media Security.
    - Malicious Code Protection.

- Assess risks:
    - Aggregate and analyze potential risks based on the type of impact.
    - Assess identified risks, ranking each for probability that the risk will materialize and the potential impact if it should occur.
    - 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:
    - Recommended risk treatment options.
    - Recommended improvements that map initiatives over a predetermined timeframe.

Deliverable

- Information Security Risk Assessment Report

3.2.2b – Information Security Risk Program Development

Based on Customer's IT risk assessment, Cisco will provide recommendations on areas for program enhancement or improvement.

Cisco Responsibilities

- Review Customer's current IT risk assessment approach, activities, and feedback, and compare to expectations.
- Current IT Risk Process Review:
  - Investigate execution effectiveness from responsible individuals.
  - Identify input and perception of process from contributors via interviews.
  - Investigate actionable outcomes and/organizational responses to IT risk assessment findings.

Deliverable

- Information Security Risk Program Development Report

3.2.3 – Third-Party Risk Assessment and Program Development

The Third-Party Risk Assessment and Program Development Service identifies potential security weaknesses in Customer's vendor and third-party Risk Management program that may result in risks to Customer. To assess effectiveness in identifying, treating, governing, and monitoring third-party risks, the assessment will review program processes.

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 plan for improvement.

Architecture Supported

- Security

3.2.3a – Third-Party Risk Assessment

Cisco Responsibilities

- Review Customer's vendor or a selected third party's Security program for potential Security weakness that may result in risks to Customer.
- Conduct an assessment that may include one of the following
  - Provide one (1) full, On Site risk assessment at one (1) third-party vendor environment.
  - Provide two (2) On Site, rapid ISO 27002 health checks at different third parties.
  - Provide two (2) Remote lightweight risk assessments against different third parties.

Deliverable

- Third-Party Risk Assessment Report

3.2.3b – Third-Party Risk Program Development

Additional Information to be Collected

- Business strategies, objectives, and initiatives dependent on third parties and related elements of overall strategy.
- Most critical third-party relationships, services, technologies, and products, and how they support Customer's business processes.
- Third-party risk management processes.

Cisco Responsibilities

- Define overall risk tolerance, and formalize business-relevant risk-rating criteria.
- Identify relevant governance, procurement, due diligence, relationship management, assurance, and risk management processes.
- Analyze areas that may include, as appropriate:
  - Third-party inventory.
  - Prioritization.
  - Requirements development.
  - Risk assessment.
  - Business continuity planning.
  - Risk-based requirements.
  - Service level agreement definition.
  - Contract standards and templates.
  - Negotiation input and impact analysis.
  - Due diligence procedures.
  - Transition and Transformation Management.
  - Performance monitoring.
  - Security and compliance assurance processes.
  - Governance structures, oversight, and accountability mechanisms.
- Evaluate sample relationships:
  - Validate Customer requirements.
  - Identify a sample of third-party relationships based on Customer prioritization and risk.
  - Perform a high-level assessment through interviews with internal stakeholders and third-party representatives to validate previous findings and identify new issues due to execution quality, which will cover:
    - Information governance and protection.
    - Compliance requirements.
    - Operational expectations.
- Evaluate business continuity and operational resilience:
  - Examine Change Management.
  - Perform a Risk Assessment.
  - Assess and prioritize risks based on business risk tolerance and agreed risk-assessment criteria.
  - Define risk profile.
- Develop Third-Party Risk Management Program Improvement Roadmap:
  - Develop an improvement roadmap based on prioritized risks, including actionable improvement recommendations and tangible interim states.

- Estimate cost, time, and resources required to implement improvement roadmap, to the extent possible.

Deliverable

- Third-Party Risk Program Development Roadmap

4—ADVANCED ANALYTICS

Advanced Analytics provides insights, recommendations, and implementation support for improving Customer application and Service ongoing strategy, architecture and design, feature selection, configuration requirements, health and performance, and Product installation or Updates.

SECTION NAVIGATION

Acceleration Theme – Advanced Analytics includes the following Service capabilities and Deliverables, each bookmarked for easier navigation:

4.1 – Application Insights

Application Insights focuses on helping Customers analyze and proactively manage the usage, health, and performance of their applications and resources to achieve their business and operational objectives.

4.1.1 – COLLABORATION APPLICATION INSIGHTS

Collaboration Application Insights provides information about how the Collaboration Solution is being used and generates standard reports in regular intervals. The reports provide insights which may be used for capacity planning, increasing adoption and optimizing the Collaboration Application and Services.

Note: This Deliverable only supports on-premise deployments of Collaboration Applications.

Architecture Supported

- Collaboration

Additional Information to be Collected

- Organization hierarchy information which contains mapping between User IDs and corresponding departments.
- Location information for different clusters.

Cisco Responsibilities

- Deliver the Collaboration Application Insights Report(s) that may include the following information:
  - Asset inventory
  - Service usage, Service quality and experience.
  - Baseline of Collaboration Solution usage pattern and trends by user, role or job function.
  - If organization hierarchy information is made available the reports can be summarized by function or department.

Deliverable

- Collaboration Application Insights Report(s)

4.1.2 – Collaboration Analytics Support

The Collaboration Analytics Support Service for Hosted Collaboration Solution (HCS) will provide the Customer with actionable data to address general platform health, known Software defects, misconfigurations, and out-of-date Software for HCS. Collectors are used to gather the data which is then analyzed using rules / thresholds / logic specific to Customer's deployment to generate summarized reports to be delivered on an agreed-upon frequency.

Technology Supported

- Hosted Collaboration Solution

Cisco Responsibilities

- Deploy Cisco Services Health and Optimization Reporting Package into the HCS environment, along with log parsing scripts necessary to support report generation.
- Configure report generation, and mail reports out at an agreed-upon frequency.
- Maintain reporting Software elements.
- Host a quarterly Platform Health and Optimization Review, in a format and schedule agreed upon by Cisco and Customer at the kickoff of Services; the review shall be limited to:
  - Review and provide recommendations on configurations that should be optimized.
  - Review Security and other vulnerabilities detected, and prioritize remediation.
  - Review known software defects, and address remediation.
  - Provide guidance on installation and configuration for installing any new Cisco Products.

Deliverable

- Health and Optimization Report

Customer Responsibilities

- Provide reporting requirements.

4.1.3 – Data Center Application Intelligence

Data Center Application Intelligence assists Customers with enhancing the resiliency, performance, and security of Customer application workloads by providing analysis of Data Center resources.

Data Center Application Intelligence provides the following deliverables:

A. Application Dependency Mapping (ADM)

B. Application Analytics Support

C. Whitelist Policy and Enforcement Guidance

Technology Supported

- Tetration

4.1.3a – Application Dependency Mapping (ADM) Support

Application Dependency Mapping (ADM) Support helps Customer review Data Center application dependencies, performance, and security by analyzing data flows and existing policies, creating application analysis views, and providing cluster / grouping recommendations for endpoints.

Additional Information to be Collected

- Customer CMDB information
- Host information and inputs for annotation

Cisco Responsibilities

- The number of applications and endpoints in scope will be specified in the quote.
- Upload inventory to Tetration Analytics and derive scope used to group access/end points for applications.
- Conduct application dependency reviews with customer.
- Provide analysis of application workloads.
- Provide templates in Tetration Analytics canonical formats of Server Load Balancing (SLB) configurations.
- Provide user-defined annotations for host inventory in comma-separated values (.CSV) format.
- Provide recommendations pertaining to clusters / groupings for endpoints being analyzed.
- Create ADM workspaces and application views per application being analyzed.
- Run live compliance analyses for published policies, per application.
- Create ADM Policy to include following (as applicable):
  - Whitelist policies between clusters
  - Micro-segmented policies
  - Endpoints within an EPG
  - Compliance analysis and recommendations
  - Application Views

Deliverable

- ADM Policy Export Report

Customer Responsibilities

- Use Tetration Analytics templates for Server Load Balancing (SLB) / Route-Tags provided by Cisco to generate configurations as required input to the ADM analysis.

Limitations

- Workload analysis not to exceed fifty (50) endpoints per application discovered with live sensors; for example, any IPv4/IPv6 address is an end point - as an input to the ADM run.
- Customer understands that if the number of endpoints per application exceeds the threshold of fifty (50), Cisco will reduce the number of Applications mapped by Cisco.
- Cisco will conduct up to three (3) reviews with Customer per application.
- Cisco will create no more than two (2) ADM workspaces per application being analyzed.
- Cisco will provide no more than three (3) application views per ADM workspace.
- Cisco will provide no more than fifteen (15) ADM runs/versions per application being analyzed.
- Cisco will run no more than three (3) live compliance analyses for published policies, per application.

4.1.3b – Application Analytics Support

Application Analytics Support assists Customers by analyzing data flows, defining and recommending policy updates, and assisting customers with updates to their ADM policies.

Cisco Responsibilities

- Analyze data flows against deployed whitelist policy.
- Analyze user defined whitelist policies.
- Update new or existing policies to incorporate new sensors into existing ADM workspace.
- Update the ADM policy based on the environment needs:
  - Create base cluster definition file for ADM runs.
  - Update sensor policy for CPU, Bandwidth.
  - Update load balancing configuration files in ADM workspaces.
- Perform one (1) of following analysis and provide recommendation for policy update:
  - Application visibility analysis
  - Data Center resources optimization analysis
  - Application reliability analysis
  - Data Center scale and redundancy analysis
  - Anomaly and outlier analysis
  - Network structure analysis
  - Traffic pattern analysis
- Work with key customer stakeholders to evaluate the impact and mitigation of observed changes in policy.
- Create compliance experiments for published Tetration policy.

Deliverable

Application Analytics Report

Limitations

The following are provided based on a frequency specified:

- Monthly
  - Update the ADM policy, analysis of user defined whitelist policies and current flow of data, analysis of data center resources and scalability, application reliability, network structure, anomaly / outliers and traffic pattern analysis.
  - Create up two (2) compliance experiments for up to one (1) published Tetration policy.
- Quarterly
  - Update sensor policy for CPU, Bandwidth.
  - Create up to one (1) base cluster definition file for ADM runs.
- Annually
  - Update load balancing configuration files in ADM workspaces.

4.1.3c – Whitelist Policy and Enforcement Guidance

Whitelist Policy and Enforcement Guidance assists Customer's implementation of a Tetration Whitelist Policy framework that is integrated with their existing Data Center application, network, security designs, policies, and configurations. Cisco will provide analysis of findings and high-level recommendations to help address design, policy, and configuration gaps.

Dependency

- Customer must have the Cisco Tetration Software Add-on License for Policy Enforcement and Application Segmentation for this Deliverable.

Additional Information to be Collected

- Active Directory (AD), Domain Name Service (DNS), and Server IP address information.
- Information specific to an existing ACI Data Center Network:
  - ACI Requirements and "as-is" Design Document
  - Data Center Policy Framework, Data Center Policy Adoption Strategy
- Information specific to Non-ACI Data Center Network:
  - Requirements and "as-is" Design Document
  - Data Center Policy Adoption Strategy

Cisco Responsibilities

- The number of applications and endpoints in scope will be specified in the quote.
- Work with customer to understand their current Data Center infrastructure environment and requirements for enforcing the Tetration Whitelist Policy within the Customer's Data Center Policy Framework.
- Cisco will provide a Whitelist Policy framework and guidance for policy enforcement that may include:
  - Micro-segmentation with end point enforcement.
  - Comparison of Tetration policy to the existing ACLs pertaining to the applications in scope.

- If applicable, Cisco will make recommendations on existing firewall rules and/or ACI contracts based on Whitelist Policies and resulting Tetration policy analysis. The recommendations will include the following, but is not limited to:
  - Unused rules and/or contracts
  - Underutilized rules and/or contracts
  - Missing rules and/or contracts
- Conduct a Customer Design Review session based only one (1) of the following:
  - Existing ACI Data Center Network
    - Comparison of the customer's requirements with Cisco Data Center ACI design, application network and security policy, application grouping, and provide high-level design recommendations to resolve gaps identified with the following:
      - Fabric Design
      - Tenant / Application Profile / End-Point Group Constructs
      - Layer 4-7 integration (Firewall and Load Balancer)
  - Non-ACI Data Center Network
    - Comparison of the customer's requirements with Cisco Data Center design, application network and security policy, application grouping, and provide high-level design recommendations to resolve gaps identified with the following:
      - Data Center L2/L3 architecture
      - Layer 4-7 integration (Firewall and Load Balancer)
- Review aspects of Customer design and deployment model including device placement, physical and logical connectivity, and network management based on Cisco leading practices.

Deliverable

- Whitelist Policy and Enforcement Guidance Report

Customer Responsibilities

- Facilitate ACL review of third-party firewalls with third-party vendor(s).
- Facilitate Policy enforcement of third-party firewalls with third-party vendor(s).

Limitations

- Cisco's Whitelist Policy framework and guidance provides Micro-segmentation with End point enforcement for up to fifty (50) End points per application.
- Cisco will participate in up to three (3), two (2) hour remote Design review session(s) over a period of two (2) weeks with Customer.

4.2 – Service Insights

Service Insights focus on helping Customers analyze and proactively manage the health and performance of their application or infrastructure Services and resources to achieve their business and operational objectives.

4.2.1 – ACI Insights

ACI Insights help improve alignment with Customer application policies and best practices, working to prioritize resource utilization proactively and support future growth requirements.

Technology Supported

- Application Centric Infrastructure

Additional Information to be Collected

- Application Policy Infrastructure Controller (APIC) data including system data, logs, Hardware and Software resources, and health scores.

Cisco Responsibilities

- Perform Fabric Performance Optimization by reviewing exceptions through analyzing system data, logs, Hardware, and Software resources collected via APIC.
- Analyze faults, relationship to managed objects, triggers, and impact on functionality.
- Perform Health Score Analysis by periodically analyzing health scores generated by APIC as well as issues impacting health scores, decipher fault codes, relationship to managed objects, triggers, and impact on functionality.

Deliverable

- Consultative guidance and support only

4.2.2 – Wi-Fi Insights

Wi-Fi Insights is adaptable to cloud-based, hybrid, and on-premise deployments. Wi-Fi Insights is an advanced Network monitoring and analysis service designed specifically to provide visibility into Cisco enterprise WLAN and third-party products and solutions. Wi-Fi Insights provide key insights based on business and operational metrics and KPIs. To aid in the communication of key metrics, Customers and/or Cisco Services Subject Matter Experts access a customizable Wi-Fi Insights Portal for the following information, but not limited to:

- Operational performance and health state of the WLAN infrastructure and mobility solution.
- Location-based information.
- Other custom data sources as agreed by Cisco delivery team, and/or information derived from any third-party integrations.

Note: The quantity, delivery frequency of the Deliverables, scope of solution, Network Elements / solution components covered, and efforts for ongoing activities will vary depending on Customer requirements and what Customer and Cisco mutually agree upon when Services are purchased.

Note: Wi-Fi Insight and Analytics feature set purchased will be specified in the Quote.

Note: Customer is responsible for the use of the Cisco-hosted Wi-Fi Insights and Analytics Portal, and other Cisco-hosted portals that may be provided as set forth in this Service Description, by Customer personnel, partners or others designated by or for Customer. Such use is subject to the Universal Cloud Terms located at http://www.cisco.com/c/en/us/products/universal-cloud-agreement.html, which is incorporated herein by reference.

Delivery of Wi-Fi Insights consists of the following two feature sets:

- Base Wi-Fi Insights and Analytics Portal Features with Wi-Fi Consulting and Support
- Premium Wi-Fi Insights and Analytics Portal Features with Wi-Fi Consulting and Support

Technology Supported

- Wireless Networking

Additional Information to be Collected

- Wi-Fi Insights use cases.
- System and application interoperability requirements.
- Network information and reports.
- Existing and planned devices, code versions, and configuration files of supported devices.
- Current and planned policies; and or key resources.
- Customer network element availability, Wi-Fi Portal KPIs to be tracked.
- Desired network performance benchmarks required for defining alerting thresholds.
- Network infrastructure elements and management tools.
- Client usage, behavior, and analytics tracking metrics.

Supported Network Elements / Solution Components for Wi-Fi Insights and Analytics Portal

Cisco-Supported Network Elements

- Cisco WLAN Controller v7.6+
- Cisco Aironet™ Wireless APs
- Cisco Prime Infrastructure v2.2+
- Cisco Mobility Services Engine (MSE) with Connected Mobile Experiences (CMX) Location Analytics v10.2.2+ or CMS Presence Analytics
- Cisco MSE with CMX Connect v10.2.2+
- Cisco Adaptive Security Appliance

Solution components may include, but are not limited to:

- Big-Data Platforms
- Analytics Algorithms
- Custom Software, Portal, and Dashboards

Cisco Responsibilities

Common Wi-Fi Insights and Analytics Portal Feature Set

- Cisco will perform the following Common Base / Premium Feature Wi-Fi Insights and Analytics Portal feature set responsibilities based on the supported Network elements / solution components in the Customer environment:
  - Customization requirements, which are different from the standard offering, would incur additional costs.
  - Validate key Customer business goals and requirements for data analytics.
  - Evaluate possible Customer cost and revenue drivers for Wi-Fi Insights visualization and consulting.
  - Identify and recommend solutions for visualizing network operational data, CMX analytics data, and customized insights.
  - Evaluate current Customer Network infrastructure including in-production analytics, data collection, and visualization platforms, as applicable.
  - Create the Customer Design Requirements Document, which may include, but is not limited to, the following:
    - Design goals and business, technical, and operational requirements.
    - Identified gaps, assessment findings, and recommendations
  - Provide descriptive, diagnostic, and predictive insights (if applicable) represented as KPIs and metrics for IT innovation and wireless operational outcomes enabled by the Wi-Fi Insights Portal dashboards.
  - Provide the Customer the Wi-Fi Insights Deployment Checklist, which is a questionnaire that captures and details the low-level technical specifications required to deploy the service within the Customer's environment.
  - Evaluate desired metrics and data sources for collection including device types, data formatting, and data collection protocols. Review Customer requirements and provide baseline and recommended metrics and data sources for collection and visualization.
  - Operate and maintain Cisco-specified cloud and/or Cisco-specified on-premise components of Wi-Fi Insights.
  - Provide ongoing Remote support for up to a number of specified hours per month per the Purchase Order.
  - Provide Wi-Fi Insights Consulting and Support, which may include, but is not limited to, the following:
    - Collected Data Analysis – Review collected KPIs, metrics, and analytics data, and filter collected data based on relevance to identify relevant insights and determine network optimization activities.
    - Periodic Monitoring – Utilizing analyzed data and management tools, proactively identify network-impacting issues, and provide recommendations and remediation steps.
    - Assist Customer in using the Wi-Fi Insights features as applicable to the delivered solution and scope.
    - Review the Network performance and the data collected from Wi-Fi Insights with Customer, and provide Wi-Fi optimization guidance and recommendations (if required).

**Specific for Base Wi-Fi Insights and Analytics Portal Feature Set:*

- In addition to the Common Wi-Fi Insights and Analytics Portal features, Cisco will perform the following based on the supported Network elements / solution components in the Customer environment:
  - Define the base Wi-Fi Insights and Analytics **P**ortal features.
  - Provide Customer with access to the following Base capabilities via the Portal(s)**,** subject to availability of and access to the required Customer network data sources:
    - Access to current and historical WLAN KPIs.
    - Detailed WLAN KPIs for each individual defined site(s) as agreed in the Power Key Encryption Server (PKES), and WLAN KPIs summarized across all sites.
    - WLAN KPIs may include RF usage, traffic throughput, traffic volume, RF channel utilization, client counts, client connection status, client device types, RF interferers, network-based application usage, and Wi-Fi user-based KPIs.
    - Traffic volume based on top applications.
    - Detailed AP inventory and performance.

Note: Customizations may include Portal naming and/or branding.

**Specific for Premium Wi-Fi Insights and Analytics Portal Feature Set*

- In addition to the Common Wi-Fi Insights and Analytics Portal Features, Cisco will perform the following based on the supported Network elements / solution components in the Customer environment:
  - Based on agreed-upon Network elements / solution components, base Wi-Fi Insights and Analytics Portal features may be provided.
  - Work with the Customer to devise specific customization requirements that may include, but are not limited to, the following:
    - Business, technical, and operational insights.
    - Advanced Analytics including **m**achine learning, predictive analytics, and prescriptive analytics.
    - Application, software, and/or dashboard customizations.
    - Custom integrations including cross-technologies, multi-architectures, and third-party solutions.
    - Big-data platforms and data feeds (API).
  - Third-party solutions supported may include, but are not limited to, the following type of network elements:
    - Customer Relationship Management Database
    - Ticketing Database

Deliverables

- Customer Design Requirements Document
- Base Wi-Fi Insights and Analytics Portal Features with Wi-Fi Insights Consulting and Support
- Premium Wi-Fi Insights and Analytics Portal Features with Wi-Fi Insights Consulting and Support

Customer Responsibilities

- **Wi-Fi Insights and Analytics Portal:**
  - Complete the Wi-Fi Insights Deployment Checklist.
  - Provide Hardware and perform configuration based on Cisco guidance for VPN tunnel setup to the Cisco-specified Cloud, where applicable. Customer should configure VPN on an endpoint available at their end. The VPN router should be able to support IPSec site-to-site tunnel to Cisco-specified data center using AES-256 encryption and pre-shared key authentication.

Note: Note: Cisco will make commercially reasonable efforts to avoid IP address overlap between Customer's onsite and off-site equipment; however, in case the address overlap occurs, Network Address Translation will be required on Customer's onsite VPN router.

  - Provide Cisco with dedicated user accounts, based on agreed permissions, to any and all devices required for On Site or Network performance monitoring.
  - Provide access to users for Cisco Wi-Fi Insights solution components, including supported browsers and versions and Network connectivity.
  - Customer shall have no right, and Customer specifically agrees not to: (a) rent, lease, distribute, sell, transfer, or sublicense its license rights to any other person, or use the Software on unauthorized or secondhand Cisco equipment; (b) make error corrections to or otherwise modify or adapt the Software nor create derivative works based upon the Software, or permit third parties to do the same; or (c) copy, in whole or in part, Software or document (except for one (1) backup copy), decompile, decrypt, reverse Engineer, disassemble, or otherwise reduce all or any portion of the Software to human-readable form. Cisco shall make available any interface information which Customer is entitled to under applicable law, upon written notice request and payment of Cisco's applicable fee.
  - Notify the Cisco Subject Matter Expert when changes are made to syslog, DNS, proxy and gateway servers IP addresses.

4.2.3 – SON Resource Analytics

SON Resource Analytics provides RAN resource balancing and management across layers and sites to reduce congestion and improve RAN KPIs.

Solution Supported

- Self-Optimizing Network
  - Mobility Policy and Access

Additional Information to be Collected

- RAN performance objectives and KPI thresholds.

Cisco Responsibilities

- Generate and review SON BI cell congestion reports at regular intervals, and have discussions with Customer on congestions and objectives.
- Analyze cell reports for High Triggers on Non-HS / HS Power Utilization, Code, and UL H / W to isolate congested cells.
- Assist Customer to optimize Mobile RAN across the layers and different cell sites by leveraging Cisco SON Inter Carrier Load Balancing (ICLB) / Dynamic Load Balancing (DLB) modules.

Deliverable

- Consultative guidance and support only

Customer Responsibilities

- Review cell congestion reports on a regular basis.
- Work with Cisco Network Consulting Engineer to configure / optimize SON modules.

4.2.4 – SERVICE ASSURANCE INSIGHTS

Service Assurance Insight provides predictive insights and correlation of performance, quality, capacity and utilization to help Customer address issues such as service degradation and sub-optimal user experience.

Service Assurance Insights provides the following:

- Performance Insights
- Capacity Insights

Exclusions

**Specific to Packet Core, Mobility Policy and Access*

- Cisco Ultra Packet Core is not supported by Service Assurance Insights Deliverables for Performance Insights and Capacity Insights.

4.2.4a – Performance Insights

Performance Insights provides analysis of top offending KPIs, correlates findings, and recommendations for remediating issues to realize performance and operational gains.

Technologies Supported

- Mobility Policy and Access
- Packet Core

Solution Supported

- Virtual Packet Core
  - Packet Core

Cisco Responsibilities

- Performance Insights consists of the following features described below:
  - Top offending performance KPIs and trends.
  - Correlation of performance KPIs impacted by alarms, syslog and threshold violations.
  - Predictive insights into performance behavior using historical trends and predictive algorithms.

Additional Responsibilities

**Specific to Technologies Supported: Packet Core, Mobility Policy and Access*

For Enhanced Package:

- Includes Intelligent Correlation Dashboards – KPI, Logs and Capacity

For Premium Package:

- Includes Enhanced Package.
- Provide machine-Learning based anomaly detection, and benchmarking.
- Update KPI, dashboards and algorithms for predictive and prescriptive advanced analytics.
- Update API(s) for integration with other Cisco domain (i.e. IP Backhaul, GiLAN, Routing and Switching) and 3rd Party nodes.
- Subscriber level analytics based on engine logs consumption for business and subscriber intelligence usage.
- Update API(s) for Integration of alerts with OSS or NMS.

Deliverable

- Portal Feature: Performance Insights

4.2.4b – Capacity Insights

Capacity Insights provides analysis of capacity trends, utilization, forecasting, predictive insights and correlation to mitigate service capacity constraints.

Technologies Supported

- Mobility Policy and Access
- Packet Core

Solution Supported

- Virtual Packet Core
  - Packet Core

Cisco Responsibilities

- Capacity Insights consists of the following features described below:
  - Top offending capacity KPIs and trends
  - Correlation of capacity KPIs impacted by resource demand and threshold violations.
  - Predictive insights into capacity behavior using historical trends and predictive algorithms.

Additional Responsibilities

**Specific to Technologies Supported: Packet Core, Mobility Policy and Access*

For Enhanced Package:

- Includes Intelligent Correlation Dashboards – KPI, Logs and Capacity

For Premium Package:

- Includes Enhanced Package.
- Provide machine-Learning based anomaly detection, capacity prediction and forecasting, and benchmarking.

- Update KPI, dashboards and algorithms for predictive and prescriptive advanced analytics.
- Update API(s) for integration with other Cisco domain (i.e. IP Backhaul, GiLAN, Routing and Switching) and 3rd Party nodes.
- Subscriber level analytics based on engine logs consumption for business and subscriber intelligence usage.
- Update API(s) for Integration of alerts with OSS or NMS.

Deliverable

- Portal Feature: Capacity Insights

5—ORCHESTRATION AND AUTOMATION

Orchestration and Automation provides assistance with adopting and supporting orchestration and automation of Service delivery, applications and workflows.

SECTION NAVIGATION

Acceleration Theme – Orchestration and Automation includes the following Service capabilities and deliverables, each bookmarked for easier navigation:

5.1 – Service Orchestration

Service Orchestration focuses on assisting Customer to successfully plan, develop, test, implement, support, and enhance Service Orchestration models and workflows to achieve their business and operational objectives.

5.1.1 – SERVICE MODEL DEVELOPMENT SUPPORT

Service Model Development Support assists Customer to accelerate the development and implementation of new Service models in an iterative DevOps environment.

Cisco will work collaboratively with Customer by embracing a DevOps lifecycle of analyzing, developing, enhancing, testing, and deploying Customer's Network Service Orchestration, Service Orchestration EMS / NMS, and Data Center capabilities and models with multiple interactions / instances.

Technologies Supported

- Network Management and Orchestration
- Data Center Orchestration and Automation

Solutions Supported

- Network Service Orchestration
  - Network Management and Orchestration
  - Data Center Orchestration and Automation

Cisco Responsibilities

- Provide Services as requested by Customer, which may include:
  - Analyze and develop new Service models in an iterative DevOps environment.
  - Assist with device configurations as part of new services.
  - Advise on YANG modeling, FastMap / Java, NED validation for NSO.

- Advise on configuration template, process workflows and provisioning flows for UCS-D, CPO, PSC, Prime Portfolio, and other Cisco EMS / NMS / Data Center Products.

Deliverable

- Consultative guidance and support only

5.1.2 – Collaboration Automation Support

Collaboration Automation provides assistance to Customer in provisioning, testing, and aligning IT requirements with business priorities and imperatives. The main objective is to help automate the configuration of Collaboration platforms, provisioning and updates of end user devices. To verify the deployment automated testing can help capture potential issues. Cisco will deploy a Cisco or third party automation tool to provide this Service.

Technology Supported

- Unified Communications

A. Provisioning Services

Provisioning Services include the automation of configuring Cisco Communications Manager (CUCM), Cisco Unity Connection, routers and switches.

Dependency

- For Collaboration provisioning automation Customer completed and finalized Low Level Design is required.
- Based on the Low Level Design, at least one branch must already be provisioned in the production environment.

Additional Information to be Collected

- Provisioning requirements for every branch site.
- Low Level Design required for writing automation scripts.

Cisco Responsibilities

- Provide remote assistance to Customer in deployment and configuration of Cisco provisioning tool(s).
- Create provisioning templates to address Customer implementation-specific requirements.
- Test and verify the accuracy of all the provisioned items for one test branch.
- Execute provisioning activities.

Deliverables

- Provisioning of Customer requested infrastructure and endpoints.

Customer Responsibilities

- Provide necessary infrastructure to implement and support the Cisco or third-party automation tool.
- Single point of contact with knowledge of Low Level Design and provisioning requirements.

B. Testing Services

Testing Services include the testing and validation of Cisco Communications Manager (CUCM) configuration and Cisco Unity Connection.

Dependency

- Validation activity starts after the Provisioning Service is completed in the production environment for each production cutover.
- Testing activity starts once the IP phones are registered and ready to make and receive calls.
- For Collaboration testing automation Customer dial plan design is required.

Cisco Responsibilities

- Provide Remote assistance to Customer in deployment and configuration of Cisco provided testing tool(s).
- Develop the Collaboration test case document to be used for validation and testing based upon Customer requirements.
- Work with Customer to schedule testing activities.

Deliverables

- Validation Results and Collaboration Testing Results Document.

Customer Responsibilities

- Provide necessary infrastructure to implement and support Collaboration Testing Services.

6—DEVELOPMENT ENGINEERING

Development Engineering provides a coordinated, streamlined approach to help Customers improve application and infrastructure readiness for growth, enhance operational productivity, ensure solution readiness, and proactively mitigate risks and threats by leveraging Cisco Services engineering expertise, intellectual property, analytics, tools, and best practices.

SECTION NAVIGATION

Acceleration Theme – Development Engineering includes the following Service capabilities and Deliverables, each bookmarked for easier navigation:

6.1 – Acceleration Trusted Advisor

Acceleration Trusted Advisor provides leadership in enabling Customers to obtain the benefits of Cisco's Acceleration capabilities with a focus on planning, coordinating, and delivering required capabilities through On Site and Remote delivery approaches.

6.1.1 – ACCELERATION ONSITE CONSULTING

Acceleration Onsite Consulting is provided at Customer's designated location up to five (5) days per week (pending local work restrictions) during Standard Business Hours, not to exceed forty (40) hours per week, excluding Cisco holidays, locally recognized country holidays, vacation, and training days.

Acceleration Onsite Consulting is only available in certain geographic locations and will be specified in the Quote for Services. The Quote will specify the primary location, period, frequency, and technologies required for Onsite Consulting.

Technologies Supported

- Routing and Switching
- Wireless Networking
- Network Management and Orchestration
- Computing Systems
- Tetration
- Data Center Orchestration and Automation
- Network Security
- Cloud Security
- Security Policy and Access
- Advanced Threat
- Unified Communications
- Customer Care
- Video Collaboration
- Cloud Meetings and Messaging
- Packet Core
- Mobility Policy and Access
- Next-Gen Cable Access
- SP Video Infrastructure

Solutions Supported

- Network Service Orchestration
  - Network Management and Orchestration
  - Data Center Orchestration and Automation
- Virtual Packet Core
  - Packet Core
- Software Defined WAN
  - Routing and Switching
  - Network Management and Orchestration

Cisco Responsibilities

- Develop an understanding of Customer's technology initiatives and requirements, and provide advice and guidance in support of Customer's objectives.
- Align Customer's objectives with the Services and Deliverables ordered by the Customer.
- Gather information and requirements through meetings with the Customer in support of planning, sequencing, and executing Deliverables.

Note:

- Cisco may deem it necessary to provide specific Deliverables through a combination of On Site consulting and Remote-support.
- Customer-directed tasks to be performed by the Cisco Network Consulting Engineer shall be governed by the Service and Deliverables ordered by the Customer and are subject to Cisco approval, which shall not be unreasonably withheld.

Additional Responsibilities

**Specific to Network Management and Orchestration, Data Center Orchestration and Automation, Network Service Orchestration*

- Assign a Cisco Engineer to represent Customer and communicate Customer's requirements to Cisco Product planning, including Software solution support and ongoing maintenance activities.

**Specific to Wireless Networking*

- Provide proactive On Site support of a Customer event utilizing a managed Cisco mobility infrastructure for end-user and spectator / participant / attendee access.
- Leverage deployed Prime Infrastructure (PI), MSE, Wi-Fi Insights Data Collection Tools, and, if applicable, Mobility Insights Portal (MIP).
- Analyze the following information:
  - KPIs.
  - Desired Network performance benchmarks.
  - Available Network infrastructure elements and management tools.
  - Client usage, behavior, and analytics tracking metrics.
- Perform the following support tasks:
  - Monitor performance and overall health of the Wireless Network for the duration of the event.
  - Provide wireless infrastructure-related troubleshooting and support during the event, to the extent possible.

  - Provide basic wireless client and end user-related troubleshooting by request during the event, to the extent possible.
- Provide Customer staff with the following assistance, capabilities, or Documentation:
  - Provide cloud-managed Cisco MIP access.
  - Provide necessary observations or recommendations before, during, and after the event.
  - Develop the Network Performance Insights Report based on collected data, analysis, and Customer-specific information.
- Provide a single, designated point-of-contact for all event-related issues throughout the course of the live event.
- Provide support to Customer stakeholders responsible for performing event tasks.
- Make available any personnel and/or access to venue as necessary for Cisco to perform event support.

Deliverables

- Deliverables supported by Onsite Consulting are based on the Acceleration Deliverables specified in the Quote for Services ordered by the Customer which may include the following:

Design and Validation	▪ Design Review ▪ Ongoing Design Support ▪ Design Development ▪ Design Change Support ▪ Validation-Test Onsite Support
Feature Engineering	▪ Advanced Feature Assessment ▪ Migration Planning and Implementation Support
Custom Integration Support	▪ Management Solution Integration Support ▪ ACI API Integration Support
Security Program Development	▪ Security Strategy Planning Support
Service Insights	▪ ACI Insights ▪ Wi-Fi Insights
Service Orchestration	▪ Service Model Development Support

Customer Responsibilities

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