Cisco Business Critical Services

Services for Engineering

This document contains the detailed description of capabilities and Deliverables aligned to Cisco Business Critical Services for Engineering.
Note: This document must be read in conjunction with the Cisco Business Critical Services General Terms.

Navigation Links:

Document Name	Link
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
Cisco Business Critical Services for Operations	https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco_Business_Critical_Services_for_Operations.pdf
Cisco Business Critical Services for Engineering	https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco_Business_Critical_Services_for_Engineering.pdf
Cisco Business Critical Services for Architecture	https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco_Business_Critical_Services_for_Architecture.pdf

TABLE OF CONTENTS

Services for Engineering Overview

Cisco Business Critical Services for Engineering provide 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 Services for Engineering theme are aligned by capabilities and supported technologies, solutions, or architectures.

Services for Engineering Capabilities and Deliverables

Services for Engineering 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

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 assists Customer with 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
- Network Function Virtualization Infrastructure (NFVI)
  - Routing and Switching
  - Data Center Switching
  - Data Center Orchestration and Automation
  - Packet Core
- Managed Services Accelerator (MSX)
  - Routing and Switching
  - Network Management and Orchestration
  - Computing Systems
- Software-Defined Access
  - Routing and Switching
  - Wireless Networking
  - Network Management and Orchestration
  - Security Policy and Access
- SP Analytics and Assurance
  - Network Management and Orchestration
- Secure Agile Exchange (SAE)
  - Routing and Switching
  - Computing Systems
  - Data Center Switching
  - Data Center Orchestration and Automation
  - Cloud Security
- Self-Optimizing Network
  - Mobility Policy and Access

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

Technologies 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

Technologies 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 assists Customer with 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.

Technologies 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.

Solutions 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 assists Customer with 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

- Software-Defined WAN
  - Routing and Switching
  - Network Management and Orchestration
- Network Service Orchestration
  - Network Management and Orchestration
  - Data Center Orchestration and Automation
- Virtual Packet Core
  - Computing Systems
  - Data Center Switching
  - Packet Core
- Network Function Virtualization Infrastructure (NFVI)
  - Routing and Switching
- Software-Defined Access
  - Routing and Switching
  - Wireless Networking
  - Network Management and Orchestration
  - Security Policy and Access
- Secure Agile Exchange (SAE)
  - Routing and Switching
  - Computing Systems
  - Data Center Switching
  - Data Center Orchestration and Automation

- Computing Systems
- Data Center Switching
- Data Center Orchestration and Automation
- Packet Core
- Cloud Security

- Managed Services Accelerator (MSX)
  - Routing and Switching
  - Network Management and Orchestration
  - Computing Systems

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:
  - Cisco CloudCenter components
  - Applications and services built with the Cisco 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
- Advanced Threat
- Packet Core

- Wireless Networking
- Network Security
- Data Center Orchestration and Automation
- Cloud Security
- Mobility Policy and Access
- Security Policy and Access

Solutions Supported

- Software-Defined Access
  - Routing and Switching
  - Wireless Networking
  - Network Management and Orchestration
  - Security Policy and Access
- Software-Defined WAN
  - Routing and Switching
  - Network Management and Orchestration
- 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

- Virtual Packet Core
- SP Analytics and Assurance

- Packet Core
- Network Management and Orchestration

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. Test Strategy and Plan Review

Test Strategy and Plan Review assists Customer 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
- Network Function Virtualization Infrastructure (NFVI)
  - Routing and Switching
  - Computing Systems
  - Data Center Switching
  - Data Center Orchestration and Automation
  - Packet Core
- Managed Services Accelerator (MSX)
  - Routing and Switching
  - Network Management and Orchestration
  - Computing Systems
- SP Analytics and Assurance
  - Network Management and Orchestration
- Secure Agile Exchange (SAE)
  - Routing and Switching
  - Computing Systems
  - Data Center Switching
  - Data Center Orchestration and Automation
  - Cloud Security

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).

1.1.6. Testing and Lab Validation Assessment

Testing and Lab Validation Assessment evaluates Customer's current test validation practices and principles for consistency and automation improvements of test plan design, development and deployment.

Architectures Supported

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

Additional Information to be Collected

- Test environment documents and test objectives.

Cisco Responsibilities

- Review Customer's validation automation environment, resources, processes, tools, concerns and challenges.
- Perform an analysis of Customer's current testing and lab validation environment for only one (1) of the following areas as specified in the Quote:
  - General Testing and Lab Validation Assessment: Review of the Customer's Lab testing environment, methodology, tools and test plan and test results practices. Identify areas of improvement of test planning guidance, best practices, recommendations for evaluating test report results.
  - Technology or Product Migration Testing and Lab Validation Assessment: Includes one (1) technology or migration specific test plan and one (1) test topology review of Customer's test plan and test results. Provide feedback and best practices recommendations.
  - Solution Testing and Lab Validation Assessment: Includes one (1) solution specific test plan and one (1) test topology review of the Customer's test plan and test results. Provide feedback and best practices recommendations.

Deliverable

- General Testing and Lab Validation Assessment Report
- Technology or Product Migration Testing and Lab Validation Assessment Report
- Solution Testing and Lab Validation Assessment Report

1.1.7. Technology Adoption and Migration Validation

Technology Adoption and Migration Validation helps Customers plan, execute, and report on the adoption of new technology test cycles. Cisco provides guidance in testing hardware, software, and architecture migration, including validation of software upgrades and method of procedures (MOP). Testing is performed in a Cisco Lab with applicable test hardware and tools. Typical technology adoption.

Architectures Supported

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

Solutions Supported

- Network Function Virtualization Infrastructure (NFVI)
  - Routing and Switching
  - Computing Systems
  - Data Center Switching
  - Data Center Orchestration and Automation
  - Packet Core
- Managed Services Accelerator (MSX)
  - Routing and Switching
  - Network Management and Orchestration
  - Computing Systems
- Secure Agile Exchange (SAE)
  - Routing and Switching
  - Computing Systems
  - Data Center Switching
  - Data Center Orchestration and Automation
  - Cloud Security

Cisco Responsibilities

- Create and document the technology adoption or migration service plan.
- Develop a Test Plan.
- Execute the tests documented in the Test Plan agreed to by Customer and Cisco.
- Provide support which includes, but is not limited to the following:
  - Test Automation – Develop and/or extend the automated test cases.
  - Test Setup and Execution – Execute the Test Plan and report finding in the Test Report.

Deliverables

- Test Plan
- Test Report

1.1.8. Continuous Automation and Integration Testing

Continuous Automation and Integration Testing provides test consulting and automated test case development for Customers requiring the redesign of their manual test cases to reusable automated test cases to accelerate new technologies, rapid deployment migrations, and new IT services. Cisco uses a Cisco automation test library and framework to develop the Customer's test cases.

Architectures Supported

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

Additional Information to be Collected

- Test plan, test case, and automation requirements and objectives.

Cisco Responsibilities

- Remotely develop automation test cases based on the Customer provided test plan.
- Review automated test cases with the Customer.
- Install and configure the Cisco Automation Validation Framework on the Customer-provided compute platform in the Customer's validation lab.
- Provide the Customer designated resources access and use of the Cisco Automation Test Library to conduct automation testing for the duration of this Service as specified in the Quote.
- Perform updates and maintenance to the Cisco automation environment.
- Execute the testing and deliver the Test Report if specified in the Quote.
- Integrate the Cisco Automated Test Library to Customer's CI/CD model if specified in the Quote.

Deliverables

- Automated Test Cases
- Test Report (if specified in the Quote)

Customer Responsibilities

- Provide specified compute platform for Cisco Automation Validation Framework Server.
- Review the automated test cases provided by Cisco.
- Setup and install the required compute platform as specified by Cisco to run the test automation environment provided by Cisco.
- Execute automation testing based on the Automated Test Plan.
- Provide Cisco with a list of Customer personnel that will have access privileges to the Cisco Automation Test Library.
- Provide Cisco detail information and resources to develop the Cisco Automated Test Library integration with the Customer's CI/CD mode, if specified in Customer's Quote.

1.1.9. Continuous Test Cycle Integration Validation

Continuous Test Cycle Integration Validation provides test validation consulting and testing for Customers requiring continuous network simulation in a Cisco Lab facility to reduce risk and accelerate the deployment of new technologies, software, hardware, security updates and other IT changes.

Architectures Supported

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

Additional Information to be Collected

- Customer's Test Plan to be automated

Cisco Responsibilities

- Review the Customer provided Test Plan.
- Provide Services that may include, among other activities, the following:
  - Test Automation – Provided the automated test cases.
  - Test Execution – Execute the Test Plan.

Deliverables

- Testing Support
- Test Plan (if specified in the Quote)

1.1.10. Onsite Test Validation Support

Onsite Test Validation Support helps Customers to adopt new technologies, implement proof of concept, or validate migration to new architectures at the Customer's premise.

Architectures Supported

- Core Networking
- Security

- Data Center and Cloud
- Collaboration
- SP Mobility

Solutions Supported

- Network Function Virtualization Infrastructure (NFVI)
  - Routing and Switching
  - Computing Systems
  - Data Center Switching
  - Data Center Orchestration and Automation
  - Packet Core
- Managed Services Accelerator (MSX)
  - Routing and Switching
  - Network Management and Orchestration
  - Computing Systems
- Secure Agile Exchange (SAE)
  - Routing and Switching
  - Computing Systems
  - Data Center Switching
  - Data Center Orchestration and Automation
  - Cloud Security
- Multicloud

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 Customer provided Test Plan.
- Provide Customer with Onsite Support for issues found during Customer's testing phase.

Deliverables

- Test Execution Report

Customer Responsibilities

- Provide installation, rack, stack and cabling of hardware, software, test, and automation tools and licenses for conducting the tests.
- Provide support, maintenance, updates, and configuration of any third-party solutions.

1.1.11. Onsite Architecture Readiness for Use Testing

Onsite Architecture Readiness for Use Testing validates the Customer's design or deployment readiness of new a (greenfield) architecture or technology with testing performed either Onsite or at a Cisco facility.

Architectures Supported

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

Additional Information to be Collected

- Test acceptance criteria for validating the Customer's design.

Cisco Responsibilities

- Create the Customer's Test Plan.
- Execute the tests in an agile method and report the findings to the Customer.

Deliverables

- Test Plan
- Test Report

Customer Responsibilities

- Access to Customer premise environment.
- Define test acceptance criteria.

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

Technologies 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 Onsite 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 offer support in evaluating Customer's solution design changes, dependencies, 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

- Routing and Switching
- Network Management and Orchestration
- Data Center Switching
- Data Center Orchestration and Automation
- Application Centric Infrastructure
- 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
- Network Function Virtualization Infrastructure (NFVI)
  - Routing and Switching
  - Computing Systems
  - Data Center Switching
  - Data Center Orchestration and Automation
  - Packet Core
- Managed Services Accelerator (MSX)
  - Routing and Switching
  - Network Management and Orchestration
  - Computing Systems
- Virtual Packet Core
  - Packet Core
- Secure Agile Exchange (SAE)
  - Routing and Switching
  - Computing Systems
  - Data Center Switching
  - Data Center Orchestration and Automation
  - Cloud Security
- Software-Defined Access
  - Routing and Switching
  - Wireless Networking
  - Network Management and Orchestration
  - Security Policy and Access

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).

Note: For a description of Cisco data collection tools and methods used refer to How Cisco Provides Services document, referenced in the BCS General Terms.

- 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.
- Determine potential, risks, or integration issues, and provide Cisco recommendations around Solution migration and risk mitigation.
- If Cisco determines it necessary, perform limited / qualified verification work in a Cisco lab to validate questions and recommendations.
- Provide consultative guidance and support to Customer with their development of 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.

Excluded Responsibilities

**Specific to Application Centric Infrastructure*

- Cisco is not responsible for application dependency mapping.

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 Application Centric Infrastructure, Data Center Switching*

- Review Method of Procedure (MOP) Documentation for pre-and-post cutover connectivity and 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

Limitation

**Specific to Application Centric Infrastructure*

- Cisco will provide a Migration Planning and Implementation Recommendation Report if Cisco determines it necessary.

**Specific to NFVI and MSX*

- Migration Planning and Implementation Support must adhere to Cisco’s published Software update paths.

1.3. Knowledge Management

Knowledge Management assists Engineering enhance technical design, development and deployment knowledge using Knowledge Transfer Sessions for Engineering, Specialized Knowledge Sessions and technical training workshops.
Note: Detailed description of Cisco Business Critical Services Learning Library and Cisco Training Knowledge Management Services is located at:
https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco_Business_Critical_Services_for_Operations.pdf

1.3.1. Knowledge Transfer Session for Engineering

Knowledge Transfer Session for Engineering provides technical information transfer on topics mutually agreeable and relevant to the design and delivery of Cisco Architecture(s), Product features and technologies within the Customer environment. Sessions focus on best practices for design, automation, analytics, deployment and adoption of Cisco Solutions. Knowledge transfers are not formal trainings or replacement for any authorized Cisco Education classes.

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
- Tetration
- Unified Communications
- Customer Care
- Video Collaboration
- Cloud Meetings and Messaging
- Hosted Collaboration Solution
- Network Security
- Cloud Security
- Security Policy and Access
- Advanced Threat
- Packet Core
- Mobility Policy and Access
- Next Gen Cable Access
- SP Video Infrastructure
- IoT Edge and Fog Compute
- Industrial Networking and Collaboration

Solutions Supported

- Network Service Orchestration
  - Network Management and Orchestration
  - Data Center Orchestration and Automation
- Virtual Packet Core
  - Packet Core
- Network Function Virtualized Infrastructure (NFVI)
  - Routing and Switching
  - Computing Systems
  - Data Center Switching
  - Data Center Orchestration and Automation
  - Packet Core
- Managed Services Accelerator (MSX)
  - Routing and Switching
  - Network Management and Orchestration
- Software-Defined WAN
  - Routing and Switching
  - Network Management and Orchestration
- Software-Defined Access
  - Routing and Switching
  - Wireless Networking
  - Network Management and Orchestration
  - Security Policy and Access
- Secure Agile Exchange (SAE)
  - Routing and Switching
  - Computing Systems
  - Data Center Switching
  - Data Center Orchestration and Automation
  - Cloud Security

- Computing Systems

Cisco Responsibilities

- Consult with Customer to identify requirements and topics for Knowledge Transfer Sessions at least forty-five (45) days in advance; Knowledge Transfer Sessions are:
  - Relevant to the Cisco Products and technologies deployed in Customer's Production Network.
  - Delivered by Cisco Services Engineer remotely using virtual web conferencing for up to four (4) hours in length with no labs and no printed course materials.
  - Delivered based on a specific number of sessions as specified in the Customer Quote.

Additional Responsibilities

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

- Record all Knowledge Transfer Sessions.
- Share session recordings with Customer for future reference.

**Specific to Packet Core*

- For Cisco Virtual Packet Core this deliverable supports RedHat OpenStack and RedHat Operating System software components.

Deliverable

- Knowledge Transfer Session Slides, if applicable.

Customer Responsibilities

- Coordinate and schedule Knowledge Transfer Sessions with a Cisco Project Manager at the beginning of each quarter.
- Provide attendees familiar with Cisco Products related to the Customer's Solution.
- Provide a maximum number of attendees at any one time that shall not exceed ten (10), unless mutually agreed upon by the Customer and Cisco.

Limitations

**Specific to Hosted Collaboration Solution*

- For the HCS Standard Service: Knowledge Transfer Sessions will be limited to two (2) sessions.
- For the HCS Premium Service: Knowledge Transfer Sessions will be limited to four (4) sessions.

1.3.2. Specialized Knowledge Session

Specialized Knowledge Session is a structured information transfer with hands-on labs (if applicable) on pre-defined topics relevant to the design and delivery of Cisco Architecture(s), Product features and technologies within the Customer environment. Sessions focus on best practices for design, programmability, configuration, automation and integration validation of Cisco Solutions. Specialized Knowledge Sessions are not a replacement for any authorized Cisco Education or Learning@Cisco classes.

1.3.2a. Specialized Knowledge Session ACI

Technologies Supported

- Application Centric Infrastructure

Additional Information to be Collected

- Overview of Customer's Cisco Products and technologies deployed relevant to the session topics.

Cisco Responsibilities

- Provides information on ACI fundamentals, configuration, basic troubleshooting techniques, migration methodologies, and pre-defined use cases for programmability, and configuration for the following:
  - ACI tenant logical structure
  - ACI policy model
  - External connectivity
  - Virtual Machine Manager (VMM) domain integration
  - Layer 4-7 Services
- Sessions are delivered by Cisco Services Engineer or a Cisco Partner as determined by Cisco.

- Provide lectures and hands-on lab.
- Provide one session of five (5) days duration for up to sixteen (16) participants at a Cisco office.

Deliverable

- Specialized Knowledge Session Slides, if applicable

1.3.2b. Specialized Knowledge Session CloudCenter

Technologies Supported

- Data Center Orchestration and Automation

Note: The following Specialized Knowledge Session responsibilities apply specifically to Cisco CloudCenter.

Cisco Responsibilities

- Provide one or more of the following sessions as specified in the quote:
- Cisco CloudCenter Overview:
- One (1) day duration, delivered remotely.
- Cisco CloudCenter Application and Services Modeling:
- Three (3) days duration, delivered remotely with hands-on lab.
- Cisco CloudCenter Administration:
- Two (2) days duration, delivered remotely with hands-on lab.
- One session is up to a maximum of ten (10) participants.

Deliverable

- Specialized Knowledge Session Slides, if applicable

Customer Responsibilities

- At least forty-five (45) days in advance of a session provide a list of participants, their role and function as it relates to the focus of the session.
- Coordinate and schedule Specialized Knowledge Sessions with a Cisco Project Manager.
- Customer is responsible for any additional costs for a remotely delivered Specialized Knowledge Session delivered at a Customer site.

1.3.2c. Specialized Knowledge Session Automation and Integration Validation Testing

Specialized Knowledge Session is a structured information transfer covering Cisco Automation and Integration Validation Testing topics relevant to the Cisco Products and Technologies deployed in the Customer's environment.

Architectures Supported

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

Cisco Responsibilities

- Overview of ROBOT test automation framework for acceptance testing and acceptance test-driven development.
- Provide Cisco best practices on automation test case development and using the Cisco Automated Test Library.
- Cisco will provide ten (10) example test cases for Customer hands-on-experience.
- Provide one (1) session of five (5) days duration for up to ten (10) participants at Customer's location during Customer's implementation phase.

Deliverable

- Specialized Knowledge Session Slides, if applicable

Customer Responsibilities

- At least forty-five (45) days in advance of a session provide a list of participants, their role and function as it relates to the focus of the session.

2. COMPLIANCE AND REMEDIATION

Compliance and Remediation assesses Customer's goals and requirements against internal and external standards for compliance, and provides analysis of findings, actionable insights, recommendations, and accelerated remediation. **Customer remains responsible for all of Customer's regulatory, legal and industry standards compliance requirements identified in this Service Description. Cisco will provide assessments and recommendations based on Cisco practices and will perform remediation tasks per Customer instruction.**

Section Navigation

Compliance and Remediation includes the following Service capabilities and Deliverables, each bookmarked for easier navigation:

2.1. Configuration Compliance

Configuration Compliance provides the Customer with an automated way of identifying devices out of compliance in the context of the Customer's policy configuration templates and industry standards. Configuration and Software Change Support reviews the Customer's planned configuration changes, software updates and provides scheduled change window support. Configuration, Software, and Regulatory Compliance and Remediation Deliverables assist the customer with an accelerated pace for remediation efforts. Customer remains responsible for determining what remediation efforts will be undertaken and whether such efforts meets Customer's requirements.

2.1.1. Policy Configuration Conformance

Policy Configuration Conformance assists Customer with insights into configuration conformance against Customer-defined policy associated with a grouping of network devices.

Technologies Supported

- Routing and Switching
- Network Security

Additional Information to be Collected

- Grouping of Network devices and associated configuration templates.
- Standard configuration template for a defined group of Network devices.

Deliverable

- Policy Configuration Conformance Report

Limitation

**Specific to Network Security*

- Policy Configuration Conformance is supported only for Cisco Adaptive Security Appliance (ASA).

2.1.2. Configuration and Software Change Support

Configuration and Software Change Support provides analysis and review of Customer's proposed changes and Method of Procedure (MOP) document for the activities in support of a planned change window. Scheduled Remote support is provided for Customer's implementation of configuration and Software changes.

2.1.2a. Configuration and Software Change Support

Additional Information to be Collected

- Related to Customer's proposed or planned changes:
  - Testing strategy, test plans and test results.
  - Change control process and schedule

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
- Tetration
- Unified Communications
- Customer Care
- Video Collaboration
- Network Security
- Cloud Security
- Security Policy and Access
- Advanced Threat
- Packet Core
- Mobility Policy and Access
- Next Gen Cable Access
- SP Video Infrastructure
- IoT Edge and Fog Compute
- Industrial Networking and

Solutions Supported

- Network Service Orchestration
  - Network Management and Orchestration
  - Data Center Orchestration and Automation
- Self-Optimizing Network (SON)
  - Mobility Policy and Access
- Network Function Virtualized Infrastructure (NFVI)
  - Routing and Switching
  - Computing Systems
  - Data Center Switching
  - Data Center Orchestration and Automation
  - Packet Core
- Managed Services Accelerator (MSX)
  - Routing and Switching
  - Network Management and Orchestration
  - Computing Systems
- Software-Defined WAN
  - Routing and Switching
  - Network Management and Orchestration
- Software-Defined Access
  - Routing and Switching
  - Wireless Networking
  - Network Management and Orchestration
  - Security Policy and Access
- Virtual Packet Core
  - Computing Systems
  - Data Center Switching
  - Packet Core
- Secure Agile Exchange (SAE)
  - Routing and Switching
  - Computing Systems
  - Data Center Switching
  - Data Center Orchestration and Automation
  - Cloud Security

Cisco Responsibilities

- Collaborate with Customer to evaluate the potential impact of the proposed scheduled change.
- Provide recommended changes to Customer's implementation plan, MOP, and test plan based on information gathered from the Customer, analysis of proposed changes, and Cisco best practices.
- Create a Change Implementation Review and Recommendation Report to document findings and recommendations, if Cisco determines necessary.
- Provide a Remote resource for critical scheduled changes.

Additional Responsibilities

**Specific to MOP Document for the following Technologies:*
Routing and Switching, Optical Networking, Wireless Networking, Computing Systems, Network Management and Orchestration, Storage Area Networking, Data Center Switching, Data Center Orchestration and Automation, Packet Core

- Provide recommended changes to Customer's implementation plan, 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:
    - Procedures performed prior to and following implementation of configuration and or Software change.
    - Rollback procedures of scheduled configuration and or Software change.

**Specific to the following Technologies and Solution:*
Network Management and Orchestration, Data Center Orchestration and Automation, Network Service Orchestration

- Provide a documented upgrade plan if applicable for toolset Product(s).
- Recommend a test plan for the upgraded tools.

**Specific to Tetration Analytics™*

- Assist in Tetration Analytics cluster upgrades, limited to one (1) upgrade per quarter.
- Assist in Sensor upgrades, limited to one (1) upgrade per quarter.

Deliverables

- Change Implementation Review and Recommendation Report (if Cisco determines necessary).
- MOP Document (specific to supported technologies).

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

Limitations

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

  **Specific to Network Management and Orchestration, Data Center Orchestration and Automation, Network Service Orchestration*
- The support contact addresses no more than three (3) support issues, identified by Customer during the change window (typically over a weekend), related to major Software installations, major site installation, and/or major configuration changes.

**Specific to MOP Document for the following technologies: Routing and Switching, Optical Networking, Wireless Networking, Network Management and Orchestration, Computing Systems, Storage Area Networking, Data Center Switching, Data Center Orchestration and Automation, Packet Core.*

- Change impact analysis is not conducted using simulation tools.
- MOPs are not provided for Cisco Software based products that require scripting.
- 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.
- MOP is not provided for migrating from one Cisco platform to another Cisco platform.

2.1.2b. Configuration and Software Change Support (HCS-Specific)

This Configuration and Software Change Support Service is specific only to the Cisco Hosted Collaboration Solution (HCS) Standard / Premium as specified in the Quote.

Technologies Supported

- Hosted Collaboration Solution

For HCS Standard:

Cisco Responsibilities

- Collaborate with Customer to evaluate the potential impact of the proposed scheduled change.
- Provide recommended changes to Customer's implementation plan, MOP, and test plan based on information gathered from the Customer, analysis of proposed changes, and Cisco best practices.
- Provide a Remote resource for critical scheduled changes.
- Provide Remote assistance for Customer to resolve critical and/or priority issues with changes during a major activity to the Production Network.

Deliverable

- Consultative guidance and support only

For HCS Premium:

Cisco Responsibilities

- Collaborate with Customer to evaluate the potential impact of the proposed scheduled change.
- Provide a MOP Document to Customer that may include the following:
  - Rollback procedures of scheduled configuration and/or Software change.
  - Procedures performed prior to and following implementation of change.
  - Change-related testing strategy, test plans, and testing results.
  - Change-impact analysis.
  - Change-control process and schedule.
- Perform the changes detailed in the MOP Document with Customer.
- Provide a Remote resource for critical scheduled changes.
- Provide Remote assistance for Customer to resolve critical and/or priority issues with changes during a major activity to the Production Network.

Deliverable

- MOP Document

2.1.3. Configuration Compliance and Remediation

Configuration Compliance and Remediation provides an automated way to help the Customer identify network devices that are out of configuration compliance, and guides the Customer through the steps to remediate / upgrade to the required standard based on recommendations outlined in Cisco Business Critical Services Best Practice Configuration or Policy Configuration Conformance Deliverables.
Configuration Compliance and Remediation provides Customer with remediation / upgrade assistance for the target Network devices using scripts based on the procedures, pre-conditions, and success criteria outlined by the Configuration and Software Change Support Deliverable.

Dependency

The following Deliverable reports are required inputs prior to creation of automation for configuration changes:

- **Platform Insights:**
  - Configuration Best Practices Recommendation Report
- **Configuration Compliance:**
  - Policy Configuration Conformance
  - Configuration and Software Change Support
  - Cisco Change Implementation Review and Recommendation Report

Technologies Supported

- Routing and Switching
- Network Security
- Wireless Networking

Note: Cisco Business Critical Services General Terms - Cisco General Responsibilities - Limitations contains the Cisco and Non-Cisco Platforms and Operations Systems supported.

Additional Information to be Collected

- Cisco Configuration Best Practices Report
- Cisco Policy Configuration Conformance Report
- Customer's completed Cisco Change Implementation Review and Recommendation Report

Cisco Responsibilities

- Create automation rules and conditions for one (1) configuration compliance standard based on procedures, pre-conditions, and success criteria outlined by Configuration and Software Change Support Deliverable, Cisco Change Implementation Review and Recommendation Report.
- Remediate the Platforms / Operating systems to the recommended best-practices policy outlined in the Cisco Best-Practices Report, or Policy Configuration Conformance Report as approved and directed by Customer.
- Provide successful job log reports.

Deliverable

- One (1) Configuration Compliance and Remediation compliance script per Platform / Operating System specified in the Quote.

Customer Responsibilities

- Complete and provide a report from one or more of the following Deliverables a pre-requisite for this Service:
  - Configuration Best-Practices Report
  - Policy Configuration Conformance Report
- Complete and provide the following report from the Cisco Configuration and Software Change Support Deliverable, a pre-requisite for this Service:
  - Change Implementation Review and Recommendation Report

2.1.4. Software Compliance and Remediation

Software Compliance and Remediation provides an automated way to help Customer identify Network devices that are out of Software compliance and guides the Customer through the steps to remediate / upgrade to the required Operating System version based on current and deployed recommended releases outlined in Software Analysis and Release Standards Report and Software Track Conformance Report.
Software Compliance and Remediation provides Customer with Software upgrade assistance using scripts for a single device or large groups of devices by utilizing the MOP, pre-check, and post-check documents that contains the pre-conditions and the post-check success criteria for all device types.

Dependency

The following Deliverable reports are required inputs prior to creation of automation for upgrades:

- **Software Lifecycle Management:**
  - Software Analysis and Release Standards Report
  - Software Track Conformance Report
- **Configuration and Software Change Support:**
  - Change Implementation Review and Recommendation Report

Technologies Supported

- Routing and Switching
- Network Security
- Wireless Networking

Note: Cisco Business Critical Services General Terms - Cisco General Responsibilities - Limitations contains Cisco and Non-Cisco Platforms and Operations Systems supported.

Additional Information to be Collected

- Customer's completed Cisco Software Analysis and Release Standards Report.
- Customer's completed Cisco Software Track Conformance Report.
- Customer's completed Cisco Change Implementation Review and Recommendation Report.

Cisco Responsibilities

- Create upgrade automation rules and conditions for one (1) Platform / Operating System.
- Upgrade the Operating System to the recommended and licensed version as outlined in the Cisco Software Analysis and Release Standards Report.
- Provide successful job log reports.

Deliverable

- One (1) software image upgrade script per Platform / Operating System specified in the Quote.

Customer Responsibilities

- Complete and provide a report from the following Deliverables a pre-requisite for this Service:
    - Software Analysis and Release Standards Report
    - Software Track Conformance Report
    - Change Implementation Review and Recommendation Report

2.1.5. Regulatory Compliance and Remediation

Regulatory Compliance and Remediation provide an automated way to help Customer identify Network devices that are out of configuration compliance in the context of industry standards (listed below).
Network Configurations are audited against rules in various categories like Routing, Switching, Wireless and Security within these standards body regulations, and results are provided per-device and aggregated.
Customers will be able to review the results to help plan maintenance windows based on their prioritization of the exceptions and Network devices. The dashboard views provide a level of detail for Network engineering staff, operations teams, auditors, and executives to view the results, trends of the audit summaries at a specified interval of a daily, weekly, monthly, or custom range.
Customer remains responsible for all of Customer's compliance requirements associated with the industry and regulatory standards identified in this Service. Cisco will provide assessments and recommendations based on Cisco practices and will perform remediation tasks per Customer instruction.

Dependency

Regulatory Compliance and Remediation is delivered with Cisco NCCM and does not depend on any reports from other Deliverables within the offer.

Usage

Customers purchase a Compliance Practices Assessment for one or more standards such as HIPAA, ISO 27002, PCI DSS, DISA DoD STIG, and other standard regulatory requirements, if available.
Regulatory Compliance and Remediation Deliverable is intended for either of the following:

- Customers who want to take the results from a Cisco Compliance Practices Assessment Deliverable and implement them in the Network based on the scope outlined below.
- Customers who want to take the results from an audit by one or more of the above-mentioned Industry Standard Regulatory bodies and implement them in the Network based on the scope outlined below.

Technologies Supported

- Routing and Switching
- Wireless Networking
- Network Security

Note: Cisco Business Critical Services General Terms - General Cisco Responsibilities - Limitations contains the Platforms and Operations Systems supported.

Cisco Responsibilities

- Perform a Compliance Device Audit via the Cisco NCCM Software for one or more of the following as specified in the Quote:
  - North American Electric Reliability Corporation (NERC)
  - NSA Security Guidelines
  - SANS Router Security Policy
  - Department of Homeland Security (DHS) Checklist
  - Security Best Practices (SAFE)
  - HIPAA Compliance
  - SOX (COBIT) Compliance
  - DISA DoD Security Technical Implementation Guides (STIG) Configuration Standards
  - DISA IOS® Checklist
  - CIS PIX and IOS Benchmark
  - FISMA Compliance
  - NIST SP800-171 Compliance
  - ISO / IEC 27002
  - Payment Card Industry Data Security Standard (PCI DSS)
- Conduct Compliance Device Audit to help identify which of Customer's deployed device configurations are non-compliant.
- Create automation rules and conditions for one (1) Platform / Operating System configuration change.
- Remediate the Cisco Platform / Operating System to the recommended best-practices policy configurations as outlined in the Compliance Device Audit.
- Provide job log reports.

Additional Responsibilities

**Specific to DISA DoD Security Technical Implementation Guides Configuration Standards Assessment*

- Perform Compliance Device Audit against STIG regulatory policies.
- Continuous Compliance Device Audit are executed based on agreed-upon schedule with Customer, such as weekly, monthly, or quarterly.
- Conduct vulnerability assessment.

Deliverables

- One (1) Compliance Device Audit based one or more of the above audits as specified in the Quote.

**Specific to DISA DoD Security Technical Implementation Guides Configuration Standards Assessment*

- In addition to the above Deliverables, the following Deliverables are provided:
  - Continuous Compliance Audits
  - DISA DoD STIG Assessment Executive Summary

2.2. Compliance Practices Assessment

Compliance Practices Assessment assesses Customer's security or regulatory compliance requirements, identifies potential gaps, and provides recommendations for remediation based on Cisco practices for Customer's consideration. Customer remains responsible for decisions related to implementing any compliance practices.

Architecture Supported

- Security

Compliance Practices Assessment consists of one or more types of compliance assessments supported by the above technologies.

- Assessment of Organization Alignment to ISO 27001
- Assessment of Organization Alignment to ISO27002
- HIPAA and HITECH Assessment
- PCI Data Security Standard (DSS) Readiness Assessment
- Security Compliance Readiness – Other Standard or Regulatory Requirement
- Security Technical Implementation Guide (STIG) Compliance Assessment

2.2.1. Assessment of Organization Alignment to ISO 27001

Cisco will perform a Compliance Practices Assessment of Customer's current alignment to ISO 27001 standard control requirements and provide Cisco's recommendations and a roadmap for preparation for ISO 27001 certification.

Additional Information to be Collected

Mandatory Documents

- Scope of the ISMS
- Information Security policy and objectives
- Risk assessment and risk treatment
- Statement of Applicability
- Risk treatment plan
- Risk assessment report
- Definition of security roles and responsibilities
- Inventory of assets
- Acceptable use of assets
- Access control policy
- Operating procedures for IT management
- Secure system engineering principles
- Supplier security policy
- Incident management procedure
- Business continuity procedures
- Statutory, regulatory, and contractual

Mandatory Records

- Records of training, skills, experience, and qualifications
- Monitoring and measurement results
- Internal audit program
- Results of internal audits
- Logs of user activities, exceptions, and security events
- Results of the management review
- Results of corrective action

Non-Mandatory (Yet Commonly Found) Documents

- Procedure for document control
- Controls for managing records
- Procedure for internal audit
- Procedure for corrective action
- Bring-your-own-device (BYOD) policy
- Mobile device and teleworking policy
- Information classification policy
- Password policy
- Disposal and destruction policy
- Procedures for working in secure areas
- Clear desk and clear screen policy
- Change-management policy
- Backup policy
- Information transfer policy
- Business impact analysis
- Exercising and testing plan
- Maintenance and review plan
- Business continuity strategy

Cisco Responsibilities

- Provide an overview of the ISO 27001 standard and the general process required to attain certification.
- Determine the scope for ISO certification:
  - Outline the in-scope processes, supporting systems, and support teams.
  - Determine if any Annex A controls may be deemed out-of-scope.
- Perform a high-level assessment of current alignment with ISO 27001 requirements.

Deliverables

- IS0 27001 Assessment Report
- ISO 27001 Assessment Executive Summary

2.2.2. Assessment of Organizational Alignment to ISO 27002

Cisco will perform a Compliance Practice Assessment to help evaluate control selection and design effectiveness and determine Customer's adherence to each domain of the ISO 27002:2013 standard. Cisco will also perform high-level effectiveness reviews of sample controls and physical site reviews of Data Centers and IT operations to help assess the operational effectiveness of controls.

Cisco Responsibilities

- Conduct a control effectiveness review to:
  - Validate control selection and design Documentation.
  - Assess operational effectiveness of controls.
  - Determine gaps in terms of information security risk.
  - Determine potential systemic risks within IT operations.
- Perform a high-level effectiveness review against sample controls via one of two methods:
  - Review of evidence of control execution and completion.
  - Observation of the control in operation.
- Perform a physical site inspection to observe implemented controls of Customer Data Centers, IT operations, and management areas at Customer's corporate headquarters.

Deliverables

- IS0 27002 Assessment Report
- ISO 27002 Assessment Executive Summary

2.2.3. HIPAA and HITECH Assessment

Cisco will perform a Compliance Practice Assessment to help determine adherence to the requirements of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, with the additional relevant requirements of the Health Information Technology for Economic and Clinical Health (HITECH) Act. The HIPAA / HITECH Security Rule Readiness Assessment will evaluate control selection and design effectiveness. Cisco will prioritize findings and map Cisco's recommended remediation efforts to provide a report that includes a HIPAA / HITECH Security Rule Readiness Roadmap.

Additional Information to be Collected

- Internal audit processes.
- Business processes and transactions that use electronic Protected Health Information (ePHI).
- Control selection and design Documentation based on HIPAA and HITECH.

Cisco Responsibilities

- Determine the scope of the assessment based on the following:
  - Physical site locations, and which controls apply at each location.
  - Relevant applications and infrastructure that store and process ePHI.
- Conduct control effectiveness review, and perform a physical site inspection to:
  - Validate control design Documentation.
  - Review operational effectiveness of controls.
  - Investigate undocumented control processes, or identify additional Documentation available for review.
- Conduct operational effectiveness review of control implementation against selected sample controls for HIPAA / HITECH requirement via one (1) of the following three (3) methods:
  - Review of evidence of control execution and completion.
  - Observation of the control in operation.
  - Assessment of control within PCI Report on Compliance (ROC) or other relevant assessment.
- Perform a physical site inspection to observe implemented controls of Customer Data Centers, IT operations, and management areas at Customer's corporate headquarters.

Deliverables

- HIPAA / HITECH Security Rule Readiness Assessment Report, including HIPAA / HITECH Security Rule Readiness Roadmap.
- HIPAA / HITECH Security Rule Readiness Assessment Executive Summary.

2.2.4. PCI-DSS Readiness Assessment

Cisco will perform a time-boxed Compliance Practices Assessment against the current PCI security standard (such as DSS 3.1) to provide insight into the current PCI compliance stance of one Cardholder Data Environment (CDE).

Additional Information to be Collected

- Control selection and design Documentation based on PCI-DSS.

Cisco Responsibilities

- Outline a plan of tactical and strategic remediation required based on findings of the assessment, including recommendations.

Deliverable

- PCI-DSS Readiness Assessment Report

Limitation

- PCI-DSS Readiness Assessment covers a sampling of devices agreed to by Customer and Cisco and is not a full ROC scan of all devices.

2.2.5. Security Compliance Readiness – Other Standard or Regulatory Requirement

Cisco will conduct a compliance gap assessment against a single security standard or regulatory requirement agreed upon by the parties.

Cisco Responsibilities

- Determine the scope of the assessment for the security standard or regulatory requirement based on the following:
  - Customer's technology environment and business processes.
  - Physical site locations, and which controls apply at each location.
- Conduct a control effectiveness review of a single security standard or regulatory requirement to:
  - Review policies and standards.
  - Validate control selection and design.
  - Validate control processes.
  - Evidence of Documentation.
  - Perform a physical site inspection to observe implemented controls at Customer Data Centers, IT operations, and management areas at Customer's corporate headquarters, if Cisco deems it applicable to the requirement.

Deliverable

- Compliance Readiness Assessment Report

2.2.6. Security Technical Implementation Guide (STIG) Compliance Assessment

STIG Compliance Assessment provides a situation awareness and compliance assessment using policies based on government compliance requirements (e.g. DOD DISA Network Infrastructure STIGs) to help assess threats to the Customer's infrastructure. Cisco's will perform Compliance Practices Assessment using compliance engine which gathers Customer's configurations, reviews them against the policies described above, and produces executive level and detailed vulnerability reports.

Additional Information to be Collected

Mandatory Documents

- Security considerations, policy and objectives.
- Risk assessment report and mitigation plan
- Statement of Applicability
- Definition of security roles and responsibilities.
- Incident management procedure
- Inventory of assets
- Acceptable use of assets
- Access control policy
- Operating procedures for IT management
- Secure system engineering principles
- Business continuity procedures
- Statutory, regulatory, and contractual

Mandatory Records

- Records of training, skills, experience, and qualifications
- Monitoring and measurement results
- Internal audit program
- Results of internal audits
- Logs of user activities, exceptions, and security events
- Results of the management review
- Results of corrective action
- Number and type of devices

Non-Mandatory (Yet Commonly Found) Documents

- Procedure for document control
- Controls for managing records
- Procedure for internal audit
- Procedure for corrective action
- Bring-your-own-device (BYOD) policy
- Mobile device and teleworking policy
- Information classification policy
- Password policy
- Disposal and destruction policy
- Procedures for working in secure areas
- Clear desk and clear screen policy
- Change-management policy
- Backup policy
- Information transfer policy
- Business impact analysis
- Exercising and testing plan
- Maintenance and review plan
- Business continuity strategy

Cisco Responsibilities

- Perform compliance audit against STIG regulatory policies. Continuous compliance audits are executed based on agreed upon schedule with Customer i.e. weekly, monthly or quarterly.
- Conduct detailed vulnerability assessment.
- Provide remediation recommendations for addressing assessment findings.

Deliverables

- Continuous Compliance Audits
- DISA DoD STIG Assessment Report
- DISA DoD STIG Assessment Executive Summary

3. APPLICATION SUPPORT

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

Section Navigation

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

3.1. Custom Application Support

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

3.1.1. 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
- Software-Defined WAN

- Network Management and Orchestration
- Data Center Orchestration and Automation

- Network Function Virtualization Infrastructure (NFVI)
  - Routing and Switching
  - Computing Systems
  - Data Center Switching
  - Data Center Orchestration and Automation
  - Packet Core
- Managed Services Accelerator (MSX)
  - Routing and Switching
  - Network Management and Orchestration
  - Computing Systems
  - Network Management and Orchestration
- SP Analytics and Assurance
  - Network Management and Orchestration
- Secure Agile Exchange (SAE)
  - Routing and Switching
  - Computing Systems
  - Data Center Switching
  - Data Center Orchestration and Automation
  - Cloud Security

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

3.1.2. 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.

Solutions 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

3.2. Custom Integration Support

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

3.2.1. 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
- Network Function Virtualization Infrastructure (NFVI)
  - Routing and Switching
  - Computing Systems
  - Data Center Switching
  - Data Center Orchestration and Automation
  - Packet Core
- Managed Services Accelerator (MSX)
  - Routing and Switching
  - Network Management and Orchestration
  - Computing Systems
- Software-Defined WAN
  - Network Management and Orchestration
- SP Analytics and Assurance
  - Network Management and Orchestration
- Secure Agile Exchange (SAE)
  - Routing and Switching
  - Computing Systems
  - Data Center Switching
  - Data Center Orchestration and Automation
  - Cloud Security

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.

3.2.2. API Support for Customer Platform Integration

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

3.2.2a. 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.

Technologies 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.

4. SECURITY PROTECTION

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

Section Navigation

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

4.1. Security Assessments

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

4.1.1. 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 Onsite 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.

4.1.2. Network Penetration Test

Network Penetration Test performs external or internal testing of a single Customer Network to assist Customer with identifying high-risk and exploitable vulnerabilities, and to provide an opportunity to measure the effectiveness of security investments against a simulated threat.

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.

4.1.3. 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.

4.1.4. Application Penetration Assessment

Application Penetration Assessment performs testing seeking 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.

4.1.5. Red Team and Purple Team

Cisco Red Team and Cisco Purple Team perform testing to gain access to Customer Network and systems. The adversarial simulation may exercise security monitoring and response capabilities and provides an opportunity to determine if Customer defenses can prevent or detect modern threats.
Definitions and interlock between teams:

Red Team is Cisco acting as an external entity to test the efficacy of security controls that are in place. This is accomplished by monitoring the behavior of real life attackers in how they target and attack an entity.
Purple Team is a combination of red team and blue team members collaborating to run through a real life attack, or select attack phases, and dissecting each action to help Customer determine how the attack can be identified and countered.
Customer (Blue Team) is the internal security entity that defends a company from malicious attacks, by attempting to identify and block an attack as it occurs. Usually separate from "normal" security teams.

Architecture Supported

- Security

Additional Information to be Collected

- Network segments and list of devices in-scope and out-of-scope for evaluating security capabilities deployed.
- Out-of-scope attack methods and targets.
- Application data protection and regulatory requirements.
- Purpose and objective(s) for post-activity data search.
- Scenarios for data filtration and code modification.

Cisco Responsibilities

- Perform intelligence gathering and vulnerability discovery where Cisco may:
  - Leverage threat intelligence to prioritize attack scenarios.
  - Utilization of Open Source Information Gathering (OSINT) techniques to identify highly exposed people, process, and technology.
- Perform exploitation activities on vulnerable environments where Cisco may:
  - Compromise system components by exploiting implementation weaknesses in software through buffer overflows, remote code execution, cross-site scripting, code injection, and other attacks.
  - Exploit operational weaknesses within patch management, configuration management, and system deployment practices.
  - Exploit user weaknesses through social engineering, password guessing, and password cracking attacks.
  - Exploit design and architectural weaknesses in wireless networks and physical security.
  - Circumvent security controls such as firewalls, intrusion detection systems, anti-virus, access controls, cryptographic protections, and data-loss prevention systems.
- Perform post-execution activities within the exploited environments where Cisco may:
  - Leverage established footholds within the organization to establish persistence.
  - Leverage established footholds within the organization to escalate privileges.
  - Move laterally within compromised systems.
  - Search for credentials and sensitive data (e.g., personally identifiable information (PII), credit card numbers).
  - Execute data filtration and code modification attacks as approved by the Customer.
- Purple Team, or Red Team for security operations, may include:
  - Evaluation of security capabilities deployed on in-scope device(s) and network segment(s).
  - Focused and repeat simulations of attacker tactics.
  - Adjusting attack tactics based on Customer feedback.

Deliverable

- The Deliverables for this Service may include one or both of the following:
- Cisco Red Team Report
- Cisco Purple Team Report

Customer Responsibilities

- Provide Cisco assistance when a required step fails which may include providing privileged access or temporarily disabling a security control.
- Provide approval one (1) week prior for Cisco to execute data filtration and code modification attacks, repeat simulation of attacker tactics.
- Provide written authorization to test as required by Cisco.
- For the Cisco Purple Team, provide Cisco access to Customer representative for up to one (1) week for each device and network segment under test.
- For the Cisco Purple Team, setup and provide Cisco local and remote access to an adequate testing environment.
- For the Cisco Purple Team, inform Cisco of preventative and detective security control information details.

- Customer's and Cisco's Red Team to mutually disclose attack and defense details.

Limitations

- The engagement may be restricted to remote attack vectors, such as attacks against Customer computers and users exposed on the Internet.
- The engagement may be restricted to on-site attack vectors, such as attacks against Customer computers and users exposed at Customer locations.
- For the Purple Team, a single device under test in a single network segment is in scope unless otherwise mutually agreed upon by Cisco and Customer.

4.1.6. Social Engineering Assessment

Social engineering Assessment seeks to identify 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.

4.2. 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.

4.2.1. 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.

4.2.2. 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.

4.2.2a. Information Security Risk Assessment

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

4.2.2b. 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

4.2.3. 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

4.2.3a. 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, Onsite risk assessment at one (1) third-party vendor environment.
    - Provide two (2) Onsite, 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

4.2.3b. 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.

5. ENGINEERING ANALYTICS

Engineering 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

Engineering Analytics includes the following Service capabilities and Deliverables, each bookmarked for easier navigation:

5.1. 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.

5.1.1. 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)

5.1.2. Collaboration Analytics Support

The Collaboration Analytics Support Service for Hosted Collaboration Solution (HCS) will provide the Customer with recommendations to address general platform health, known Software defects, misconfigurations, and out-of-date Software for HCS. Data Collection Tools 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.

Technologies 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.

5.1.3. 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:

- Application Dependency Mapping (ADM)
- Application Analytics Support
- Whitelist Policy and Enforcement Guidance

Technologies Supported

- Tetration

5.1.3a. 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/endpoints 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 endpoint - 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.

5.1.3b. 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.

5.1.3c. 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 endpoint 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.

5.2. 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.

5.2.1. 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.

Technologies Supported

- Application Centric Infrastructure
- Network Security

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.

5.2.2. SON Resource Analytics

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

Solutions 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.

5.3. Performance and Capacity

Performance and Capacity provides near-real time predictive insights and correlation of performance, quality, capacity and utilization data to help Customer address issues such as service degradation and sub-optimal user experience.
Performance and Capacity provides the following Deliverables:

- Performance and Capacity Insights
- Performance Tuning Support
- Performance Benchmarking Analytics
- Performance Intelligence Analytics
- Capacity Assessment

5.3.1. Performance and Capacity Insights

Performance and Capacity Insights provides near-real time and automated analysis of top offending KPIs, utilization, trends, correlated findings, and recommendations for remediating issues to realize performance and capacity gains.

Exclusions

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

- Cisco Ultra Packet Core is not supported by Performance Insights and Capacity Insights.

Technologies Supported

- Mobility Policy and Access
- Packet Core

Solutions Supported

- Virtual Packet Core
  - Packet Core

Cisco Responsibilities

- Performance and Capacity Insights consists of the following features described below:
  - Top offending performance and capacity KPIs and trends.
  - Correlation of performance and capacity KPIs impacted by alarms, resource demand, syslog or threshold violations.
  - 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 and Capacity Insights

5.3.2. Performance Tuning Support

Performance Tuning Support (PTS) assesses gaps with performance objectives, policies, and configurations, and assists Customer with recommended tuning changes for performance, security, and resiliency.

Technologies Supported

- Wireless Networking
- Network Management and Orchestration
- Data Center Orchestration and Automation
- Network Security
- Cloud Security
- Security Policy and Access
- Advanced Threat
- IoT Edge and Fog Compute
- Industrial Networking and Collaboration

Solutions Supported

- Network Service Orchestration
  - Network Management and Orchestration
  - Data Center Orchestration and Automation
- Network Function Virtualization Infrastructure (NFVI)
  - Routing and Switching
  - Computing Systems
  - Data Center Switching
  - Data Center Orchestration and Automation
  - Packet Core
- Managed Services Accelerator (MSX)
  - Routing and Switching
  - Network Management and Orchestration
  - Computing Systems
- Software-Defined WAN
  - Routing and Switching
  - Network Management and Orchestration
- Secure Agile Exchange (SAE)
  - Routing and Switching
  - Computing Systems
  - Data Center Switching
  - Data Center Orchestration and Automation
  - Cloud Security

Exclusion

**Specific to Data Center Orchestration and Automation*

- Cisco CloudCenter (CCC) is not supported.

Additional Information to be Collected

- Performance gaps, tuning requirements, strategies, and concerns.

Cisco Responsibilities

- Analyze policy implementation and alignment with corporate policies and procedures and Cisco best practices.
- Analyze system features and configuration for optimizing performance and resiliency.
- Recommend areas that may need further analysis, such as architecture and design, ongoing policy compliance, configuration management, and instrumentation management (if Cisco determines necessary).

Additional Responsibilities

**Specific to Wireless Networking*

- Conduct on site data collection and Customer-specified use-case testing.
- Provide one (1) interactive tuning session with Customer to implement recommendations.
- Assist Customer with testing and validating changes.

Deliverable

- Performance Tuning Report

Limitations

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

- Security PTS is not intended for complex systems and Solutions, such as: Cisco ISE environments, Cisco Secure ACS deployments, and Network devices supporting complex 802.1x deployments.
    - Each unit of Security PTS includes up to one (1) solution set or one (1) service device type:
        - One (1) solution set (e.g., firewall solution, VPN solution, Intrusion Prevention System [IPS]), which consists of:
            - Up to five (5) devices within given solution set for the first Security PTS unit.
            - Up to five (5) additional devices for additional Security PTS units.
            - If a new solution set is added; for example, if the Security PTS includes firewall and VPN solutions, then two Security PTS units allow up to ten (10) firewall and/or VPN devices to be analyzed and tuned.
        - Up to fifteen (15) additional devices for additional Security PTS units.
            - If the solution set does not change; for example, if the Security PTS includes a VPN solution, then two Security PTS units allows up to twenty (20) VPN devices to be analyzed and tuned.
    - One (1) Security device type (e.g., multi-purpose Security devices supporting firewall, VPN, IPS), which consists of:
        - Up to two (2) security devices.

**Specific to NFVI, SAE, MSX*

- Performance Tuning Support is not provided for any Third-Party Virtualized Network Functions (VNFs).

5.3.3. Performance Benchmarking Analytics

Performance Benchmarking Analytics Service provides Customer with a report of key performance indicators (KPI), benchmarks, actionable recommendations, and improvements to Network performance and quality.

Technologies Supported

- Packet Core

Solutions Supported

- Virtual Packet Core
    - Packet Core

Cisco Responsibilities

- Develop a comparative Network Benchmarking Report based on similar number of nodes and similar call-model profiles in peer Networks to help bring focus and attention to areas of improvement from a Network performance perspective; based on the domain coverage, the report may include the following:
    - Control Plane KPIs and/or User Plane KPIs.
    - Review of observations and findings.
    - Recommend actionable items to improve Network quality.

Deliverable

- Network Benchmarking Report

5.3.4. Performance Intelligence Reports

The Performance Intelligence Reports Service provides Customer with an analysis of top offending system and application KPIs, correlate findings, and offer recommendations for remediating issues to realize performance and operational gains.

Technologies Supported

- Packet Core

Solutions Supported

- Virtual Packet Core
    - Packet Core

Cisco Responsibilities

- Develop a report that will include a list of key Network indicators based on the subscribed domain specified in the Quote for Services; the report will provide consolidated views and thresholds, and may include the following:
  - Holistic view of Network performance.
  - Identification of top offending KPIs and trends.
  - Recommended remediation steps based on detected offending indicators.
  - Preemptive indication of problematic indicators.
  - Correlation of other data sources such as syslogs / configurations / SNMP trap errors.
  - Synchronization of detected errors based on known issues found within the Cisco knowledge base.

Deliverable

- Performance Intelligence Report

5.3.5. Capacity Assessment

Capacity Assessment establishes a baseline used to analyze the impact of current and planned growth, and provides Customer with recommendations to align with capacity requirements.

Technologies Supported

- Optical Networking
- Network Management and Orchestration
- Data Center Orchestration and Automation
- Hosted Collaboration Solution
- Packet Core

Solutions Supported

- Network Service Orchestration
  - Network Management and Orchestration
  - Data Center Orchestration and Automation
- Network Function Virtualization Infrastructure (NFVI)
  - Routing and Switching
  - Computing Systems
  - Data Center Switching
  - Data Center Orchestration and Automation
  - Packet Core
- Virtual Packet Core
  - Packet Core
- Secure Agile Exchange (SAE)
  - Routing and Switching
  - Computing Systems
  - Data Center Switching
  - Data Center Orchestration and Automation
  - Cloud Security
- Managed Services Accelerator (MSX)
  - Routing and Switching
  - Network Management and Orchestration
  - Computing Systems

Exclusion

**Specific to Data Center Orchestration and Automation*

- Cisco CloudCenter (CCC) is not supported.

Additional Information to be Collected

- Planned changes related to growth, downsizing, and/or consolidation of infrastructure and applications resources.
- Bandwidth capacity, traffic profile utilization trends, recent upgrades, changes, and any future plans.

Cisco Responsibilities

- Provide recommendations for optimal deployment and configurations based on information gathered and analysis of findings; recommendations may include, but are not limited to:
  - Reference architecture highlighting capacity growth options based on Cisco best practices.
  - Tuning changes that optimize resource utilization.
  - Best practices for monitoring Network and component utilization.

- Published scaling limits for Cisco-deployed Hardware.

Deliverable

- Capacity Assessment Report

Limitation

**Specific to Optical Networking*

- The scope of the Capacity Assessment is limited to slot, interface and wavelength availability for nodes which are reachable via remote access. Circuit level capacity is out of scope.

**Specific to NFVI, SAE, MSX*

- Capacity Assessment only supports tuning changes that optimize resource utilization.

6. ORCHESTRATION AND AUTOMATION

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

Section Navigation

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

6.1. 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.

6.1.1. 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, Cloud 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
- Network Function Virtualization Infrastructure (NFVI)
  - Routing and Switching
  - Computing Systems
  - Data Center Switching
  - Data Center Orchestration and Automation
  - Packet Core
- Secure Agile Exchange (SAE)
  - Routing and Switching
  - Computing Systems
  - Data Center Switching
  - Data Center Orchestration and Automation
  - Cloud Security
- Managed Services Accelerator (MSX)
  - Routing and Switching
  - Network Management and Orchestration
  - Computing Systems

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.
  - Software implementation support as listed in the Quote and as referenced in the "Additional Responsibilities" section below
  - 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 and Cloud Products.

Additional Responsibilities

**Specific to Business Process Automation and Automation Service Packages*

- As specified in the Quote.
- Software implementation support for:
  - Implementation Core Platform High Availability (Optional)
  - Implementation High Availability+ Disaster Recovery (Optional)
  - Implementation of Service Packages (Optional)
  - Lab Environment (Optional)
  - Solution Staging Environment (Optional)

**Specific to Multicloud Domain*

As specified in the Quote.

- Software Implementation support for:
  - Nexus and ACI components
  - Hyperflex Data Platform using Cisco Intersight
  - Integrate with one (1) Public Cloud Provider
  - CSR1000v
  - CloudCenter Suite
  - Cisco Container Platform (CCP) on Hyperflex
  - Cisco Workload Optimization Manager from OVA as follows:
  - Integrate with Stealthwatch Cloud

Deliverable

- Consultative guidance and support only.

7. RESIDENT ENGINEERING EXPERT

Resident Engineering Expert provides Customers with Engineering Onsite Consulting for engineering initiatives in support of the design and delivery of Cisco solutions, technology architectures, service orchestration and automation, infrastructure and application analytics, operational security risk, and protection strategies.

Section Navigation

Resident Engineering Expert includes the following Service capabilities and Deliverables, each bookmarked for easier navigation:

7.1. Trusted Advisor

Trusted Advisor provides leadership in enabling Customers to obtain the benefits of Cisco Business Critical Services for Engineering capabilities with a focus on planning, coordinating, and delivering required capabilities through Onsite and Remote delivery approaches.

7.1.1. Engineering Onsite Consulting

Engineering Onsite Consulting is provided at Customer's designated location up to five (5) days per week (pending local work restrictions) during Standard Business Hours.

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

- Software-Defined WAN
  - Routing and Switching
  - Network Management and Orchestration
- Network Service Orchestration
  - Network Management and Orchestration
  - Data Center Orchestration and Automation
- Virtual Packet Core
  - Packet Core
- Network Function Virtualization Infrastructure (NFVI)
  - Routing and Switching
  - Computing Systems
  - Data Center Switching
  - Data Center Orchestration and Automation
  - Packet Core
- Secure Agile Exchange (SAE)
  - Routing and Switching
  - Computing Systems
  - Data Center Switching
  - Data Center Orchestration and Automation
  - Cloud Security
- Managed Services Accelerator (MSX)
  - Routing and Switching
  - Network Management and Orchestration
  - Computing Systems

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 Onsite 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 Onsite support of a Customer event utilizing a managed Cisco mobility infrastructure for end-user and spectator / participant / attendee access.
- Leverage deployed Cisco Prime® Infrastructure (PI), MSE, 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 Services for Engineering 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 • Onsite Test Validation Support • Onsite Architecture Readiness for Use Testing
Feature Engineering	• Advanced Feature Assessment • Migration Planning and Implementation Support
Knowledge Management	• Knowledge Transfer Session for Engineering
Configuration Compliance	• Policy Configuration Conformance • Configuration and Software Change Support • Configuration Compliance and Remediation • Software Compliance and Remediation
Custom Integration Support	• Management Solution Integration Support • ACI API Integration Support
Security Program Development	• Security Strategy Planning Support
Service Insights	• ACI 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.