CISCO BUSINESS CRITICAL SERVICES

FOUNDATION THEME

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

**Note:** This document must be read in conjunction with the [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 GENERAL TERMS


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

**CISCO BUSINESS CRITICAL SERVICES FOUNDATION THEME**


**CISCO BUSINESS CRITICAL SERVICES ACCELERATION THEME**


**CISCO BUSINESS CRITICAL SERVICES TRANSFORMATION THEME**

## TABLE OF CONTENTS

**CISCO BUSINESS CRITICAL SERVICES** ........................................................................................................... 1
  - CISCO BUSINESS CRITICAL SERVICES GENERAL TERMS ................................................................. 1
  - CISCO BUSINESS CRITICAL SERVICES FOUNDATION THEME .................................................... 1
  - CISCO BUSINESS CRITICAL SERVICES ACCELERATION THEME ................................................... 1
  - CISCO BUSINESS CRITICAL SERVICES TRANSFORMATION THEME ............................................. 1

**TABLE OF CONTENTS** ................................................................................................................................. 2

**FOUNDATION THEME OVERVIEW** .............................................................................................................. 5

**FOUNDATION THEME CAPABILITIES AND DELIVERABLES** ............................................................................. 6

### 1—FOUNDATIONAL ANALYTICS .................................................................................................................. 6

Section Navigation ............................................................................................................................................... 6

1.1 – Health Insights ......................................................................................................................................... 7
  1.1.1 – PLATFORM INSIGHTS ....................................................................................................................... 7
    1.1.1a – Platform Insights, Type 1 - Manual or Cisco Data Collection Tool Delivered Reports .................. 7
    1.1.1b – Platform Insights, Type 2 – Cisco Cloud Hosted Analytics and Insights Portal Delivered Features 13
    1.1.1c – Platform Insights, Type 3 – Cisco OnPrem Analytics and Insights Tool Delivered Reports ......... 18
  1.1.2 – PERFORMANCE TUNING SUPPORT ................................................................................................. 19
  1.1.3 – PERFORMANCE BENCHMARKING ANALYTICS .............................................................................. 20
  1.1.4 – PERFORMANCE INTELLIGENCE REPORTS ..................................................................................... 21
  1.1.5 – AUTOMATED FAULT MANAGEMENT ............................................................................................... 21
  1.1.6 – SERVICE MONITORING AND REPORTING ..................................................................................... 22

1.2 – Technology Assessments ......................................................................................................................... 23
  1.2.1 – RESILIENCY ASSESSMENT ............................................................................................................... 23
  1.2.2 – CAPACITY ASSESSMENT .................................................................................................................. 25
  1.2.3 – NETWORK DEVICE SECURITY ASSESSMENT ................................................................................... 26
  1.2.4 – COLLABORATION SECURITY ASSESSMENT .................................................................................. 26
  1.2.5 – RADIO FREQUENCY VERIFICATION ASSESSMENT ...................................................................... 28
  1.2.6 – WLAN RADIO FREQUENCY ASSESSMENT ................................................................................... 28
  1.2.7 – VALIDATION TESTING AND LAB STRATEGY ASSESSMENT ......................................................... 29

### 2—COMPLIANCE AND REMEDIATION ............................................................................................................. 30

Section Navigation ............................................................................................................................................... 30
2.1 – Security Compliance ................................................................................................................................... 31
  2.1.1 – SECURITY COMPLIANCE ASSESSMENT ............................................................................................................................... 31
  2.1.1a – Assessment of Organization Alignment to ISO 27001 ..................................................................................... 31
  2.1.1b – Assessment of Organizational Alignment to ISO 27002 .................................................................................. 32
  2.1.1c – HIPAA and HITECH Assessment ....................................................................................................................... 33
  2.1.1d – PCI-DSS Readiness Assessment ....................................................................................................................... 34
  2.1.1e – Security Compliance Readiness – Other Standard or Regulatory Requirement ............................................. 34

2.2 – Software Compliance and Remediation ..................................................................................................... 36
  2.2.1 – CONFIGURATION AND SOFTWARE CHANGE SUPPORT ........................................................................................................... 36
  2.2.1a – Configuration and Software Change Support ................................................................................................. 36
  2.2.1b – Configuration and Software Change Support (HCS-Specific) .......................................................................... 38
  2.2.2 – SOFTWARE LIFECYCLE MANAGEMENT .............................................................................................................................. 39
  2.2.2a – Software Lifecycle Management, Type 1 – Manual or Cisco Data Collection Tool-Delivered Reports ........... 40
  2.2.2b – Software Lifecycle Management, Type 2 – Cisco Cloud Hosted Analytics and Insights Portal Delivered Features ........................................................................................................................................................................ 44
  2.2.2c – Software Lifecycle Management, Type 3 – Cisco OnPrem Analytics and Insights Tool-Delivered Reports .... 49
  2.2.3 – SOFTWARE COMPLIANCE AND REMEDIATION ..................................................................................................................... 51
  2.2.4 – CONFIGURATION COMPLIANCE AND REMEDIATION .............................................................................................................. 52
  2.2.5 – REGULATORY COMPLIANCE AND REMEDIATION .................................................................................................................. 53

3—OPERATIONAL PROFICIENCY ....................................................................................................... 56

Section Navigation ............................................................................................................................................... 56

3.1 – Instrumentation Management ................................................................................................................... 57
  3.1.1 – MANAGEMENT INSTRUMENTATION REVIEW ...................................................................................................................... 57
  3.1.2 – MANAGEMENT DEPLOYMENT PLANNING AND READINESS ASSESSMENT ................................................................................... 58

3.2 – Metrics Management ................................................................................................................................. 58
  3.2.1 – KPI DEFINITION, IMPLEMENTATION, AND REPORT .............................................................................................................. 58
  3.2.2 – KPI AUDIT AND RECOMMENDATION ................................................................................................................................ 59
  3.2.3 – KPI TRENDING AND REPORTING ...................................................................................................................................... 60
  3.2.4 – MAPPING OPERATIONAL METRICS TO BUSINESS OUTCOMES ................................................................................................. 61
  3.2.5 – SECURITY METRICS PROGRAM DEVELOPMENT ................................................................................................................... 61

3.3 – Operations Management............................................................................................................................ 62
  3.3.1 – OPERATIONS RISK MANAGEMENT ASSESSMENT ................................................................................................................... 62
  3.3.2 – OPERATIONS RISK REMEDIATION ................................................................................................................................ 63
Main Navigation: Foundation Theme

3.3.3 – OPERATIONS PROCESS OR RUN BOOK UPDATE ................................................................................................................... 64
3.3.4 – IT OPERATIONS MODEL ANALYSIS ................................................................................................................................... 64
3.3.5 – ESCALATION ENGINEERING SUPPORT ................................................................................................................................ 65
3.3.6 – ASSET MANAGEMENT .................................................................................................................................................. 66
3.3.7 – INCIDENT MANAGEMENT .............................................................................................................................................. 67
3.3.8 - PROBLEM MANAGEMENT .............................................................................................................................................. 68
3.3.8a – Problem Management - High-Touch Technical Support ................................................................................. 68
3.3.8b – Problem Management - High-Touch Engineering ...................................................................................................................... 69
3.4 – Knowledge Management ........................................................................................................................................... 70
3.4.1 – KNOWLEDGE TRANSFER SESSION ..................................................................................................................................... 70
3.4.2 – SPECIALIZED KNOWLEDGE SESSION .................................................................................................................................. 71
  3.4.2a – Specialized Knowledge Session ....................................................................................................................... 71
  3.4.2b – Specialized Knowledge Session ....................................................................................................................... 72
3.4.3 – CYBER RANGE WORKSHOP ............................................................................................................................................ 73
3.4.4 – LEARNING LIBRARY .......................................................................................................................................................... 73
  3.4.4a. – Technical Knowledge Library ......................................................................................................................... 74
  3.4.4b – Cisco Platinum Learning Library ...................................................................................................................... 75
3.4.5 – CISCO TRAINING .......................................................................................................................................................... 75
  3.4.5a – Cisco Open Enrollment Training ...................................................................................................................... 75
  3.4.5b – Cisco Closed Enrollment Private Group Training ............................................................................................ 76
3.5 – Classified Network (U.S. Only) ........................................................................................................................................... 76
  3.5.1 - CLASSIFIED NETWORK SUPPORT ...................................................................................................................................... 76
    3.5.1a – CNS High-Touch Operations Management (U.S. Only) ................................................................................... 77
    3.5.1b - CNS High-Touch Technical Support (U.S. Only) ............................................................................................... 79
4—THREAT MITIGATION ................................................................................................................................................... 83
7. Section Navigation ........................................................................................................................................... 83
4.1 – Security Incident Response ........................................................................................................................................... 83
  4.1.1 – INCIDENT RESPONSE RETAINER ..................................................................................................................................... 83
5—RELIABILITY ENGINEERING ................................................................................................................................................... 85
7. Section Navigation ........................................................................................................................................... 85
5.1 – Foundation Trusted Advisor ................................................................................................................................................... 85
  5.1.1 – FOUNDATION ONSITE CONSULTING .................................................................................................................................. 85
  5.1.2 – FOUNDATION ONSITE SUPPORT ................................................................................................................................... 87
The **Foundation theme** of Cisco Business Critical Services provides capabilities and Deliverables in support of availability, performance, security compliance, and management of Cisco infrastructure and application environment. Deliverables described in the Cisco Business Critical Services Foundation theme are aligned by capabilities, and supported technologies, solutions or architectures.

The below diagram is for illustrative purposes only.
FOUNDATION THEME CAPABILITIES AND DELIVERABLES

Foundation capabilities and Deliverables assist Customers with optimizing operations and management of the Network infrastructure and application technologies.

1—FOUNDATIONAL ANALYTICS

Foundational Analytics provides analysis and insights into system, Software, and operational gaps that must be addressed to optimize performance, availability, and security of the Cisco Network and application architecture.

SECTION NAVIGATION

Foundation Theme – Foundational Analytics includes the following Service components, each bookmarked for easier navigation:

- **1.1 – Health Insights**
  - 1.1.1 – Platform Insights
    - Platform Insights, Type 1 - Manual or Cisco Data Collection Tool Delivered Reports
    - Platform Insights, Type 2 - Cisco Hosted Portal Delivered Features
    - Platform Insights, Type 3 - Cisco OnPrem Tool Delivered Reports
  - 1.1.2 – Performance Tuning Support
  - 1.1.3 – Performance Benchmarking Analytics
  - 1.1.4 – Performance Intelligence Reports
  - 1.1.5 – Automated Fault Management
  - 1.1.6 – Service Monitoring and Reporting

- **1.2 – Technology Assessments**
  - 1.2.1 – Resiliency Assessment
  - 1.2.2 – Capacity Assessment
  - 1.2.3 – Network Device Security Assessment
  - 1.2.4 – Collaboration Security Assessment
  - 1.2.5 – Radio Frequency Verification Assessment
  - 1.2.6 – WLAN Radio Frequency Assessment
  - 1.2.7 – Validation-Testing and Lab Strategy Assessment
1.1 – Health Insights

Health Insights is analysis and insights against best practices to identify gaps and provide recommendations to optimize operations of the Cisco technology.

1.1.1 – Platform Insights

Platform Insights identifies deficiencies and potential risks that should be resolved to optimize availability, stability, and performance of Customer’s Cisco infrastructure and application environment. The service also helps assess the effectiveness of the Cisco environment for purposes of planning current and future changes based on Customer’s evolving business imperatives and requirements.

Service involves collection and analysis of data on post-deployment or audited environments that require regularly planned or additional examination, guided by Customer needs and concerns.

Exclusions

*Specific to Wireless Networking
  - Cisco Meraki™ networking is not supported.

*Specific to Computing Systems
  - Cisco HyperFlex is not supported.

*Specific to Data Center Switching
  - Cisco Application Control Engine (ACE) is not supported.

*Specific to Automation, Integration and Management
  - Cisco CloudCenter (CCC) is not supported.

*Specific to Security Policy and Access
  - Cisco Firepower Management Center (FMC), and Identity Services Engine (ISE) are not supported.

1.1.1a – Platform Insights, Type 1 - Manual or Cisco Data Collection Tool Delivered Reports

Platform Insights Type 1 provides the following reports:

- Type 1 Configuration Best Practices
- Type 1 Hardware Lifecycle Milestones
- Type 1 Diagnostic Analysis
- Type 1 Field Notices (where applicable)
- Type 1 Audit
Type 1 Configuration Best Practices

Technologies Supported

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

Solutions Supported

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

Deliverable

- Type 1 Configuration Best Practices Report

Limitation

*Specific to Routing and Switching

- Questionnaire and/or worksheet are the only data collection methods supported for gathering information as input to the Configuration Best-Practices Report.
- One (1) Configuration Best Practices Report supports up to five (5) device configurations.

*Specific to Optical Networking

- One (1) Configuration Best Practices Report supports up to fifty (50) device configurations.
- Scope of Configuration Best Practices Report is limited to optical power level thresholds only.

*Specific to Virtual Packet Core

- For Virtual Packet Core solution one (1) Configuration Best Practices Report supports up to five (5) device configurations.
Type 1 Hardware Lifecycle Milestones

Technologies Supported

- Routing and Switching
- Optical Networking
- Wireless Networking
- Computing Systems
- Storage Area Networking
- Data Center Switching
- Network Security
- Cloud Security
- Security Policy and Access
- Advanced Threat
- SP Video Infrastructure
- Next Gen Cable Access

Solutions Supported

- Software Defined WAN
  - Routing and Switching
- Virtual Packet Core
  - Computing Systems
  - Data Center Switching

Deliverable

- Type 1 Hardware Lifecycle Milestones Report

Limitations

*Specific to Routing and Switching

- Questionnaire and/or worksheet are the only data collection methods supported for gathering information as input to the Hardware Lifecycle Milestones Report.
- One (1) Hardware Lifecycle Milestone Report supports a maximum of one hundred (100) devices.

*Specific to Optical Networking

- One (1) Hardware Lifecycle Milestone Report supports a maximum of fifty (50) devices.

Type 1 Diagnostic Analysis

Technologies Supported

- Optical Networking
- Computing Systems
- Storage Area Networking
- Data Center Switching
- Network Security
- Cloud Security
- Security Policy and Access
- Advanced Threat
- Packet Core
- SP Video Infrastructure
- Next Gen Cable Access

Solution Supported

- Virtual Packet Core
  - Computing Systems
  - Data Center Switching
  - Packet Core
Cisco Responsibilities

- Analyze Customer device diagnostic information to identify potential risks.

Additional Cisco Responsibilities

*Specific to Packet Core, Virtual Packet Core Solution excluding Computing Systems and Data Center Switching

- Analyze syslog information to develop recommendations based on the following:
  - Syslog event correlation, mobility packet core health information and baseline metrics

*Specific to Optical Networking

- Analyze syslog information to develop recommendations based on the following:
  - Alarms and conditions, system resources and shelf environment

Deliverable

- Type 1 Diagnostic Analysis and Recommendation Report

Limitation

*Specific to Optical Networking

- One (1) Diagnostic Analysis and Recommendation Report supports a maximum of fifty (50) devices.
- Scope of Diagnostic Analysis and Recommendation Report is limited to alarm and circuit information, user activities, provisioning and maintenance access information.

Type 1 Field Notices (where applicable)

Technologies Supported

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

Solutions Supported

- Software Defined WAN
  - Routing and Switching
- Virtual Packet Core
  - Computing Systems
  - Data Center Switching
  - Packet Core

Deliverable

- Type 1 Field Notice Analysis and Recommendation Report
Limitations

*Specific to Routing and Switching*
- Questionnaire and/or worksheet are the only data collection methods supported for gathering information as input to the Field Notice Analysis and Recommendation Report.
- One (1) Field Notice Analysis and Recommendation Report supports a maximum of one hundred (100) devices.

*Specific to Optical Networking*
- One (1) Field Notice Analysis and Recommendation Report supports a maximum of fifty (50) devices.

Type 1 Audit

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

Solutions Supported
- Network Service Orchestration
  - Network Management and Orchestration
  - Data Center Orchestration and Automation
- Virtual Packet Core
  - Computing Systems
  - Data Center Switching
  - Packet Core
- SP Analytics and Assurance
  - Network Management and Orchestration

Cisco Responsibilities
- Analyze information that may include, but is not limited to:
  - Performance, and tuning recommendations.
  - Resource utilization analysis for planning purposes.
- Recommend areas that need further analysis, such as architecture and design or alignment of policies and standards.

Additional Responsibilities

*Specific to Application Centric Infrastructure*
- Gather Customer’s working practices for maintaining ACI architecture.
Excluded Responsibilities

*Specific to Computing Systems, Data Center Switching

- The audit analysis and report do not address:
  - Stability, performance, and tuning recommendations.
  - Resource utilization analysis for planning purposes.

Deliverable

- Type 1 Audit Report

Customer Responsibilities

- Complete platform audit questionnaire and/or worksheet, if applicable.
- Perform any necessary pre-audit steps requested by Cisco to ensure that all data is accessible during the audit.
- Provide notification of any delay in scheduled changes during the audit process.

Limitations

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

- Type 1 Audit Report is limited to:
  - Up to one (1) Solution set or one (1) complex system (e.g., Cisco Identity Services Engine (ISE), Cisco Secure Access Control System (ACS), 802.1x deployments).
  - Up to twenty (20) devices.

*Specific to Data Center Switching

- One (1) Type 1 Audit Report is limited to Cisco Nexus® family switches in a single instance of Data Center.

*Specific to Optical Networking

- One (1) Type 1 Audit Report supports a maximum of fifty (50) devices.
- Scope of Type 1 Audit Report is limited to IP Addressing and Data Communications Network (DCN), and Dense Wave Division Multiplexing (DWDM) channel utilization.
1.1.1b – Platform Insights, Type 2 – Cisco Cloud Hosted Analytics and Insights Portal
Delivered Features

**Exclusions**

*Specific to Computing Systems*
- UCS C-Series servers not connected to Fabric Interconnect are not supported by Platform Insights, Type 2 Deliverables.

*Specific to Packet Core, Mobility Policy and Access*
- Cisco Ultra Packet Core is not supported by Platform Insights, Type 2 Deliverables.

Platform Insights Type 2 provides the following features and report:

- Type 2 Standard Portal Feature: Configuration Best Practices
- Type 2 Standard Portal Feature: Hardware Lifecycle Milestones
- Type 2 Standard Portal Feature: Diagnostic Analysis
- Type 2 Standard Portal Feature: Field Notices
- Type 2 Optional Policy Configuration Conformance
- Type 2 Audit Report
- Type 2 Optional Portal Feature: Third Party Support

**Type 2 Standard Portal Feature: Configuration Best Practices**

**Technologies Supported**
- Routing and Switching
  - Wireless Networking
  - Packet Core
  - Network Security
- Data Center Switching
  - Storage Area Networking
  - Mobility Policy and Access

**Solution Supported**
- Virtual Packet Core
  - Data Center Switching

**Deliverable**
- Type 2 Standard Portal Feature: Configuration Best Practices

**Limitation**

*Specific to Wireless Networking*
- Type 2 Standard Portal Feature: Configuration Best Practices is supported only for Cisco Autonomous Access Points.

*Specific to Network Security*
- Type 2 Standard Portal Feature: Configuration Best Practices is supported only for Cisco Adaptive Security Appliance (ASA).
**Type 2 Standard Portal Feature: Hardware Lifecycle Milestones**

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

**Solution Supported**
- Virtual Packet Core
  - Computing Systems
  - Data Center Switching

**Deliverable**
- Type 2 Standard Portal Feature: Hardware Lifecycle Milestones

**Limitation**

*Specific to Network Security, Security Policy and Access*
- Type 2 Standard Portal Feature: Hardware Lifecycle Milestones is supported only for Cisco Adaptive Security Appliance (ASA), Firepower, Firepower Threat Defense (FTD), and Identity Services Engine (ISE).

**Type 2 Standard Portal Feature: Diagnostic Analysis**

**Technologies Supported**
- Routing and Switching
- Computing Systems
- Storage Area Networking
- Data Center Switching
- Network Security
- Packet Core
- Mobility Policy and Access

**Solution Supported**
- Virtual Packet Core
  - Computing Systems
  - Data Center Switching

**Additional Responsibilities**

*Specific to Packet Core, Mobility Policy and Access*
- The following diagnostic insights packages are provided:
  - **For Base package:**
    - Network health summary for GTPC call flows, KPIs, and procedures such as Attach, PDP/Bearer Creation, Routing Area/Tracking Area Update, Paging, Service Requests and Handover Requests where applicable.
    - Resource level summary of CPU and memory utilization.

Session and throughput trends, resource utilization.
- Congestion packet drops, retransmissions, timeouts for all interfaces and Access Point Names (APNs).
- Interface level summary of sessions, transactions, diameter call flows where applicable.
- Syslog summary of Top N syslog events, critical, error and info syslog event trends.

**Deliverable**
- Type 2 Standard Portal Feature: Diagnostic Analysis

**Limitation**
*Specific to Network Security*
- Type 2 Standard Portal Feature: Diagnostic Analysis is supported only for Cisco Adaptive Security Appliance (ASA).

**Type 2 Standard Portal Feature: Field Notices**

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

**Solution Supported**
- Virtual Packet Core
  - Computing Systems
  - Data Center Switching

**Deliverable**
- Type 2 Standard Portal Feature: Field Notice Analysis and Recommendation Report

**Limitation**
*Specific to Network Security, Security Policy and Access*
- Type 2 Standard Portal Feature: Field Notices is supported only for Cisco Adaptive Security Appliance (ASA), Firepower, Firepower Threat Defense (FTD), and Identity Services Engine (ISE).

**Type 2 Optional Portal Feature: Policy Configuration Conformance**

**Technology 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
- Type 2 Optional Portal Feature: Policy Configuration Conformance

Limitation
*Specific to Network Security*
- Type 2 Optional Portal Feature: Policy Configuration Conformance is supported only for Cisco Adaptive Security Appliance (ASA).

**Type 2 Audit Report**

**Technologies Supported**
- Routing and Switching
- Computing Systems
- Packet Core
- Data Center Switching
- Storage Area Networking
- Mobility Policy and Access

**Solution Supported**
- Virtual Packet Core
  - Computing Systems
  - Data Center Switching

**Cisco Responsibilities**
- Analyze information which may include, but is not limited to:
  - Stability, performance, and tuning recommendations.
  - Resource utilization analysis for planning purposes.
  - Recommendation related to areas that need further analysis, such as architecture and design or alignment of policies and standards.

**Excluded Responsibilities**
*Specific to Computing Systems, Data Center Switching, Virtual Packet Core Computing Systems and Data Center Switching*
- The audit analysis and report do not address:
  - Stability, performance, and tuning recommendations.
  - Resource utilization analysis for planning purposes.

**Deliverable**
- Type 2 Audit Report

**Limitation**
*Specific to Data Center Switching*
- One (1) Type 1 Audit Report is limited to Nexus family switches in a single instance of Data Center.
Type 2 Optional Portal Feature: Third Party Support

Third Party Support provides Customer an inventory view of the Cisco supported third party platforms and Operating systems via Cisco Cloud Hosted Analytics and Insights Portal.

**Limitation**

- SNMP MIB-2 support by the third party device vendor is required to collect inventory data. The accuracy and completeness of the data collected by Cisco is dependent on the third party vendor support for SNMP MIB-2.
- Cisco is not responsible for the appropriateness and reliability of any information collected or provided by a third party vendor’s device(s), website or any other sources of information.
- Cisco is not responsible for the availability, performance, security or reliability of third party devices Customer requests Cisco to collect data and report on.

**Technologies Supported**

- Routing and Switching
- Wireless Networking
- Network Security

**Third Party Operating Systems and Platforms Supported**

<table>
<thead>
<tr>
<th>Company</th>
<th>Operating Systems</th>
<th>Platforms Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adtran</td>
<td>AOS</td>
<td>Adtran – NetVanta 3200</td>
</tr>
<tr>
<td>Alcatel</td>
<td>SROS</td>
<td>Alcatel 7750 Services Routers</td>
</tr>
<tr>
<td>Alteon</td>
<td>AlteonOS</td>
<td>Alteon Application Switch 2208</td>
</tr>
<tr>
<td>Arista</td>
<td>EOS</td>
<td>Arista 7050 Switches</td>
</tr>
<tr>
<td>Aruba</td>
<td>Aruba OS</td>
<td>Aruba Wireless Line Controller</td>
</tr>
<tr>
<td>BoSS</td>
<td>BoSS</td>
<td>BS470-48T, ER54550T, BS551048T</td>
</tr>
<tr>
<td>Checkpoint</td>
<td>IPSO GAIA</td>
<td>Checkpoint Firewall IPxxx</td>
</tr>
<tr>
<td>Extreme</td>
<td>EXOS</td>
<td>Extreme Summit Switches</td>
</tr>
<tr>
<td>Forti</td>
<td>FortiOS</td>
<td>Forti – Analyzer 60D, Manager</td>
</tr>
<tr>
<td>F5</td>
<td>TMOS</td>
<td>F5 – VIPRION C2400 Series, BIG IP</td>
</tr>
<tr>
<td>Huawei</td>
<td>VRP</td>
<td>Huawei S3328 Switches</td>
</tr>
<tr>
<td>Infoblox</td>
<td>NIOS</td>
<td>Infoblox 1552-A</td>
</tr>
<tr>
<td>Juniper</td>
<td>JunOS ScreenOS</td>
<td>Juniper - M Series, SRX240 Services Gateway, EX2200</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NetScaler</td>
<td>NetScalerOS</td>
<td>Citrix NetScaler, NetScaler SDX</td>
</tr>
</tbody>
</table>
Cisco Responsibilities

- Provide an inventory view of Customer third party devices within Cisco Cloud Hosted Insights and Analytics Portal which may include the following:
  - Chassis, IP Address, device type, device name, software / firmware versions

Deliverable

- Type 2 Optional Portal Feature Third Party Support

Customer Responsibilities

- Customer is responsible for resolving data issues with data collected by Cisco from the third party device vendor.
- In order for Cisco to provide this Service, Customer is responsible for providing expertise on third party vendor’s platforms such as but not limited to:
  - Hardware nomenclature
  - Features and configuration commands
  - Software versions
  - Access methods and credentials
- Customer must maintain and monitor the availability, performance, security and reliability of third party devices supported by Cisco data collection method; including ensuring configurations and software versions on third party devices deployed in the Customer environment are not misconfigured or contain defects which are affected by Cisco data collection methods.
- Customer should contact Cisco Sales representative for additional third party platforms and features not currently listed.

1.1.1c – Platform Insights, Type 3 – Cisco OnPrem Analytics and Insights Tool Delivered Reports

Technology Supported

- Routing and Switching
- Data Center Switching
- Network Security
- Security Policy and Access

Deliverables

- Type 3 Configuration Best Practices Report
- Type 3 Hardware Lifecycle Milestones Report
- Type 3 Field Notice Analysis and Recommendation Report (where applicable)

Limitation

*Specific to Network Security, Security Policy and Access

- Type 3 Configuration Practices Report is supported only for Cisco Adaptive Security Appliance (ASA).
- Type 3 Hardware Lifecycle Milestones Report is supported only for Cisco Adaptive Security Appliance (ASA), Firepower, Firepower Threat Defense (FTD), and Identity Services Engine (ISE).
- Type 3 Field Notice Analysis and Recommendation Report is supported only for Cisco Adaptive Security Appliance (ASA), Firepower, Firepower Threat Defense (FTD), and Identity Services Engine (ISE).
1.1.2 – PERFORMANCE TUNING SUPPORT

Performance Tuning Support (PTS) assesses gaps with performance objectives, policies, and configurations, and provides 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
- Software Defined WAN
  - Routing and Switching
  - Network Management and Orchestration

**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 allow 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.

1.1.3 – PERFORMANCE BENCHMARKING ANALYTICS

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

Technology Supported

- Packet Core

Solution 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
1.1.4 – PERFORMANCE INTELLIGENCE REPORTS

The Performance Intelligence Reports provide 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

**Solution 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

1.1.5 – AUTOMATED FAULT MANAGEMENT

Automated Fault Management analyzes device syslogs using Cisco rules and algorithms to detect Software, Hardware, and configuration faults in the Network, and deliver remediation instructions to the Customer. Historical trends and predictive algorithms can identify impending faults. Syslogs are monitored near-real time to detect sequences that indicate a fault has happened or is imminent. When detection occurs, the system may collect device data required for problem resolution, which may result in a notification and / or opening a case with Cisco support.

**Technology Supported**
- Routing and Switching

**Cisco Responsibilities**
- Explain system deployment and operational requirements.
- Configure and deploy Automated Fault Management virtual machine (VM) in Customer’s Network to process syslogs and open support cases.
Inform Customer of one or more of the following when fault detection has occurred:
- Notification of faults detected
- Any collected data
- Suggested remediation steps
- Support cases

Update managed device information on the Automated Fault Management server based on Customer-supplied information (as often as once per week).

Deliverable
- Quarterly Faults Detected and Service Request Status Report

Customer Responsibilities
- Provide specified deployment and runtime environment for Cisco Automated Fault Management Server VM.
- Provide Cisco Automated Fault Management Server with communications access to devices under Service for collection of configuration and status data.
- Provide Cisco Automated Fault Management Server with encrypted communications access to Cisco-hosted servers for the purpose of support case management and Software Updates to Automated Fault Management Software.
- Provide Cisco with device list and access credentials for all Network devices under Service, and update said list promptly when Network changes occur; this information may be supplied via API to Cisco Network Collector device, if present, or by formatted electronic record provided to Cisco personnel.
- Configure devices under Service to send syslog messages to a syslog server. Configure syslog server to forward the syslog events to Automated Fault Management VM.
- Provide access to email server for Automated Fault Management Server. Provide email addresses for notification emails.
- Integrate alarm management system with Cisco Automated Fault Management using Rest API, if desired; Cisco will not perform this work.

1.1.6 – SERVICE MONITORING AND REPORTING

Service Monitoring and Reporting provides operations best practices, data-driven insights and KPIs related to incidents for improvements to service quality, service performance and operational efficiency gains.

Dependency
- Service Monitoring and Reporting requires purchase of Incident Management Deliverable.
- Reporting of Root Cause Analysis and Recommendations requires purchase of Problem Management Deliverable.

Solution Supported
- High-Touch Expert Care
Additional Information to be Collected

- Established processes and procedures used for support.

Cisco Responsibilities

- Provide status and reporting, escalation assistance, and coordinate the return of parts requiring Engineering Field Analysis (“EFA”).
- Review status and progress of Service Delivery levels, open Service Requests, follow-up on actions and address outstanding issues.
- Conduct a quarterly review of Deliverables and activities provided during the immediate past timeframe and actions planned for the next quarter.
- Conduct regular proactive operations excellence assessments.
- Create Customer profile for Cisco Technical Services knowledge of Customer’s operations processes, procedures, and network access for support.
- Provide Service Incident Reporting which may include the following as applicable:
  - Cisco Service Requests, Known Errors, Post Incident Operational Improvements, Root Cause Analysis and Recommendations, Operational Abnormalities and Trends.
  - KPI and Analytics reporting focused on analytics to improve operational efficiency

Deliverables

- EFA Coordination and Reporting
- Service Delivery Level Reporting
- Incident Management Readiness Assessment
- Service Incident Reporting
- Analytics and KPI Dashboard Reports

1.2 – Technology Assessments

Technology Assessments identify gaps and provide recommendations for optimizing the capacity, reliability, general performance, and/or security of Cisco technologies.

1.2.1 – Resiliency Assessment

The Resiliency Assessment evaluates the resiliency and availability for enabling secure, reliable, high-quality Network and application services. The assessment focuses on resiliency and availability improvements to the architecture and operations of the Cisco technology.

Technologies Supported

- Routing and Switching
- Optical Networking
- Data Center Switching
- Network Security
- Cloud Security
- Security Policy and Access
- Advanced Threat
- SP Video Infrastructure
Solution Supported

- Software Defined WAN
  - Routing and Switching

Additional Information to be Collected

- Baseline of current availability and impact from service interruptions.

Cisco Responsibilities

- Recommend improvements, primarily focusing on availability and resiliency; improvements may include, but are not limited to:
  - Design and configuration changes.
  - Monitoring features.
- Provide a roadmap and an agreed-upon priority for resiliency improvements.

Deliverable

- Resiliency Assessment Report

Limitations

The following limitations are specific only to the technology listed.

- **Routing and Switching:**
  - Resiliency Assessment covers only Cisco Routing and Switching networking devices (up to 5000 Cisco devices).
  - Cisco Wi-Fi Hardware and Software lifecycles along with manageability and security best practices are included in the analysis. Wi-Fi specific configurations and Radio Frequency (RF) studies are not covered in the Routing and Switching Resiliency Assessment; these activities are supported within the WLAN RF Assessment Deliverable.
  - Cisco Firewall and load-balancer Hardware and Software lifecycles are included in the analysis, but Firewall and load-balancer rules are not included.
  - VoIP configurations are out-of-scope.
  - Third-party equipment is out-of-scope.
  - Resiliency Assessment analyzes and makes recommendations addressing the existing Network infrastructure, and does not make recommendations based on future Network designs.
  - Resiliency Assessment does not offer any Network performance analysis, application analysis, or Network bandwidth utilization assessments.

- **Network Security; Cloud Security; Security Policy and Access; Advanced Threat:**
  - Each unit of Resiliency Assessment includes:
    - Up to one (1) security technology (such as Cisco ISE, Cisco AnyConnect® Remote VPN, or 802.1x deployments).
    - Up to two (2) Network segments with a total of up to ten (10) Customer device classes, defined as a group of devices (such as firewalls or routers) that have what Cisco reasonably determines to be similar configurations.
SP Video Infrastructure:
- Resiliency Assessment performed for SP Video Infrastructure will focus on End-User Availability Assessment, and does not assess the entire Network availability.

Optical Networking:
- One (1) Resiliency Assessment Report supports a maximum of fifty (50) devices.
- The scope of the Resiliency Assessment will focus on protection schemes and alternate routing at the hardware level only. Resiliency of power plant, circuit and node capacity, and third-party products is out of scope.

1.2.2 – CAPACITY ASSESSMENT

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

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

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

Exclusion
*Specific to Data Center Orchestration and Automation
- Cisco CloudCenter (CCC) is not supported.

Additional Information to be Collected
- 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.

1.2.3 – NETWORK DEVICE SECURITY ASSESSMENT

Network Device Security Assessment analyzes device configurations and firewall rules to identify gaps and provide recommendations for remediation.

**Technologies Supported**

- Network Security
- Cloud Security
- Security Policy and Access
- Advanced Threat

**Additional Information to be Collected**

- Customer’s device security templates, device configurations, and policies.

**Cisco Responsibilities**

- Assess up to 350 Cisco device configurations; only ten (10) of those devices may be firewalls.
- Analyze device configurations, focusing on configuration security hardening of the individual devices.
- Analyze firewall rules for common configuration issues.

**Deliverable**

- Network Device Security Assessment Report

1.2.4 – COLLABORATION SECURITY ASSESSMENT

Collaboration Security Assessment provides Customer with a Security Assessment Report, recommendations, and risk analysis of five critical Solution elements:

- **Collaboration Network Infrastructure**: Network Segmentation / VLANs, quality of service, Access Control Lists, Hardware and Software, DHCP, DNS, TFTP, and NTP.
- **ID & Access Management**: access privilege, account management, access logging, configuration change management
- **Call Control**: Cisco Unified Communications Manager (CUCM), Voice gateways, SIP trunks, Cisco Unified Border Element (CUBE), dial plan, signaling, and media.
- **Endpoints**: Cisco Unified IP phones, soft phones, Video endpoints, and devices that connect to the IP Network.
- **Applications**: User applications such as CUCM, Unified Messaging, Conferencing, Video, Customer Care, and custom tools extend the capabilities of IP communications systems.

**Technology Supported**

- Unified Communications
Additional Information to be Collected

*Specific to Collaboration Security*

- UC infrastructure, which may include the following:
  - Historical CUCM call detail records
  - Dial-plan report and log(s) report
  - Analysis of CUCM call routing
  - Media and signaling protection
  - Endpoints
  - Applications
  - Voice Gateway, SIP Trunk / CUBE data
- Customer Care infrastructure, which may include the following:
  - Windows Operating System (OS) Server
  - MS SQL Server
  - Windows Firewall / Ports
  - Anti-virus
  - Remote Desktop
- Video Collaboration infrastructure, which may include the following:
  - Video applications
  - Call control
  - Conferencing
  - Video endpoints
  - Collaboration edge

Cisco Responsibilities

The scope of the Collaboration Security Assessment will focus on one or both of the following areas specified in the Quote:

- Toll Fraud
- Telephony Denial of Service (TDoS)

Customer Requirements Validation

- Verify Customer’s selected Collaboration Solution endpoints and security concerns.
- Confirm application servers and hosting location, along with Customer security concerns.
- Validate Collaboration Solution deployment model (physical and logical) and security requirements (if any).
- Verify any federated connections or business-to-business applications running in the Network.
- Verify PSTN (SIP) trunking and security applied, as applicable.

Security Assessment

- Assess the effectiveness of Network security controls intended to protect the Customer Collaboration Solution.
- Perform Software risk analysis on Collaboration application servers and endpoints.
Analyze and compare Customer security policies with Cisco leading Collaboration security best practices.

Conduct analyses on CUCM and voice gateways or SIP trunks, as applicable.

**Deliverables**

- Collaboration Security Assessment Report
- Collaboration Security Assessment Executive Summary

**Customer Responsibilities**

- No major changes are made to the Collaboration infrastructure while the Security Assessment is in progress, which may take up to four (4) weeks depending on the complexity of the environment.

### 1.2.5 – RADIO FREQUENCY VERIFICATION ASSESSMENT

The Radio Frequency (RF) Verification Assessment surveys the RF environment and provides an analysis and recommendations for optimal RF performance and coverage.

**Technology Supported**

- Wireless Networking

**Additional Information to be Collected**

- Measurements of internal / external interference at one moment in time.

**Cisco Responsibilities**

- Validate RF performance and coverage of the WLAN against the documented WLAN design.
- Survey the RF environment for coverage, interference, general performance, and Network configuration.

**Deliverable**

- RF Verification Document

### 1.2.6 – WLAN RADIO FREQUENCY ASSESSMENT

WLAN RF Assessment works to identify RF signal propagation for optimizing wireless access point (AP) placement. Cisco performs an On Site survey to capture and evaluate site details, including physical and environmental considerations, electrical and AC / DC supplies, cabling, Network synchronization, peripheral equipment, and remote access.

**Technology Supported**

- Wireless Networking

**Cisco Responsibilities**

- Conduct an On Site survey of the RF environment for coverage, interference, general performance, and Network configuration.
- Perform critical RF survey to determine the optimal AP placement.
- Develop recommendations for site modification and improvements by performing analyses that include:
  - RF Coverage Analysis.
  - Interference Analysis.
  - RF Spectrum Analysis (Optional).

**Deliverable**

- Site Survey Report

### 1.2.7 – Validation Testing and Lab Strategy Assessment

Validation Testing and Lab Strategy Assessment Service helps develop an overall strategy for Solution validation and testing in a Customer lab.

**Architectures Supported**

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

**Additional Information to be Collected**

- Test environment documents and test objectives.

**Cisco Responsibilities**

- Review Customer’s test environment, resources, concerns, and challenges.
- Perform analysis of Customer’s current Solution testing, test automation practices, and lab strategy.

**Deliverable**

- Lab Strategy Assessment Report
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 automated 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

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

- 2.1 – Security Compliance
  - 2.1.1 – Security Compliance Assessment
- 2.2 – Software Compliance and Remediation
  - 2.2.1 – Configuration and Software Change Support
  - 2.2.2 – Software Lifecycle Management
    - Software Lifecycle Management, Type 1 Manual or Cisco Data Collection Tool Delivered Reports
      - Type 1 Software Management Process and Procedure Development
      - Type 1 Software Release Standards and Conformance
      - Type 1 Software Risk Management and Insights
    - Software Lifecycle Management, Type 2 Cisco Cloud Hosted Analytics and Insights Portal Delivered Features
      - Type 2 Software Management Process and Procedure Development
      - Type 2 Software Release Standards and Conformance
      - Type 2 Software Risk Management and Insights
    - Software Lifecycle Management, Type 3 Cisco OnPrem Analytics and Insights Tool Delivered Reports
      - Type 3 Software Management Process and Procedure Development
      - Type 3 Software Release Standards and Conformance
      - Type 3 Software Risk Management and Insights
  - 2.2.3 – Software Compliance and Remediation
  - 2.2.4 – Configuration Compliance and Remediation
  - 2.2.5 – Regulatory Compliance and Remediation
2.1 – Security Compliance

Security Compliance assesses Customer’s security goals and compliance requirements, identifies gaps, and provides recommendations for remediation.

2.1.1 – Security Compliance Assessment

Architecture Supported

- Security

Security Compliance Assessment consists of one or more types of the Security Compliance Assessments supported by the above technologies. The quantity and type of Security Compliance Assessment(s) purchased by Customer will be specified in the Quote for Services.

A. Assessment of Organization Alignment to ISO 27001
B. Assessment of Organization Alignment to ISO27002
C. HIPAA and HITECH Assessment
D. PCI Data Security Standard (DSS) Readiness Assessment
E. Security Compliance Readiness – Other Standard or Regulatory Requirement

2.1.1a – Assessment of Organization Alignment to ISO 27001

Cisco will perform a Security Compliance Assessment of Customer’s current alignment to ISO 27001 standard control requirements, and provide 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 methodology
- Statement of Applicability
- Risk treatment plan
- Risk assessment report
- Definition of security roles and responsibilities
- Inventory of assets
- Acceptable use of assets
- Access control policy
- Operating procedures for IT management
- Secure system engineering principles
- Supplier security policy
- Incident management procedure
- Business continuity procedures
- Statutory, regulatory, and contractual requirements
Mandatory Records

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

Non-Mandatory (Yet Commonly Found) Documents

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

- ISO 27001 Assessment Report
- ISO 27001 Assessment Executive Summary

2.1.1b – Assessment of Organizational Alignment to ISO 27002

Cisco will perform a Security Compliance Assessment to 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 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

- ISO 27002 Assessment Report
- ISO 27002 Assessment Executive Summary

2.1.1c – HIPAA and HITECH Assessment

Cisco will perform a Security Compliance Assessment to determine adherence to the requirements of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, with the additional relevant requirements of the Health Information Technology for Economic and Clinical Health (HITECH) Act. The HIPAA / HITECH Security Rule Readiness Assessment will evaluate control selection and design effectiveness. Cisco will prioritize findings and map 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 Executive Summary.

### 2.1.1d – PCI-DSS Readiness Assessment

PCI-DSS Readiness Assessment is a time-boxed assessment performed by Cisco 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.

### 2.1.1e – 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

### 2.1.1f – 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 compliance engine 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 requirements

**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

2.2 – Software Compliance and Remediation

Software Compliance and Remediation provides insights for planning of Software features and release updates. It also proactively assists with identifying optimum Software release standards and automating Software, configuration, and/or regulatory compliance remediation.

2.2.1 – 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.

2.2.1a – 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 Collaboration
Solutions Supported

- Network Service Orchestration
  - Network Management and Orchestration
  - Data Center Orchestration and Automation
- Self-Optimizing Network (SON)
  - Mobility Policy and Access
- Software Defined WAN
  - Routing and Switching
  - Network Management and Orchestration
- Virtual Packet Core
  - Computing Systems
  - Data Center Switching
  - Packet Core

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.

Note: Upon receipt of not less than twenty-one (21) days prior written request to Cisco by Customer, Cisco will work with Customer to identify a designated support contact person who will be available to consult with Customer on major Service changes, such as major Hardware upgrades, major site installations, or major configuration and/or Software 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

- 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:


- 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.

2.2.1b – 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.

Note: Upon receipt of not less than twenty-one (21) days prior written request to Cisco by Customer, Cisco will work with Customer to identify a designated support contact person who will be available to consult with Customer on major Service changes, such as major Hardware upgrades, major site installations, or major configuration and/or Software 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.

Note: Upon receipt of not less than twenty-one (21) days prior written request to Cisco by Customer, Cisco will work with Customer to identify a designated support contact person who will be available to consult with Customer on major Service changes, such as major Hardware upgrades, major site installations, or major configuration and/or Software 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

2.2.2 – SOFTWARE LIFECYCLE MANAGEMENT

Software Lifecycle Management assists Customer with preparing and planning future Software release decisions such as feature functionality, third-party compatibility, and release stability, aligned with Customer’s future Software release objectives. It also analyzes Customer’s current practices related to establishing and managing release standards, working to identify risks and provide insights to help prevent potential issues.
General Limitations

The following limitations apply specifically to bugs identified in Production Software Maintenance Updates (SMUs) by Software Lifecycle Management Deliverables described below and Cisco’s discretion regarding requests for and delivery of Production SMUs:

- Production Software Maintenance Updates (SMU) are provided on Customer request on supported maintenance releases for service impacting issues observed in production or during maintenance release validation, for which there is no feasible workaround.
- Software bugs identified through software recommendations or Bug Search Tools are not a basis for Production SMU request.
- Cisco reviews software bugs affecting supported maintenance releases and provides Proactive Production SMU requests when Cisco deems necessary.
- Cisco reserves the right to maintain strict control over Production SMU delivery.

Exclusion

*Specific to Wireless Networking
- Cisco Meraki networking is not supported.

*Specific to Computing Systems
- Cisco HyperFlex is not supported.

*Specific to Data Center Switching
- Cisco Application Control Engine (ACE) is not supported.

2.2.2a – Software Lifecycle Management, Type 1 – Manual or Cisco Data Collection Tool-Delivered Reports

Software Lifecycle Management Type 1 consists of the following three (3) areas of focus:

- **Type 1 Software Management Process and Procedure Development**
- **Type 1 Software Release Standards and Conformance**
- **Type 1 Software Risk Management and Insights**

Type 1 Software Management Process and Procedure Development

**Technologies Supported**

- Routing and Switching
- Optical Networking
- Wireless Networking
- Network Management and Orchestration
- Data Center Orchestration and Automation
- Unified Communications
- Video Collaboration
- Customer Care
- Cloud Meetings and Messaging
- Network Security
- Cloud Security
- Security Policy and Access
- Advanced Threat
- 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
- Software Defined WAN
  - Routing and Switching
  - Network Management and Orchestration
- SP Analytics and Assurance
  - Network Management and Orchestration

Cisco Responsibilities

- Collaborate with Customer to develop the Software Management Process and Procedure Document, which may include:
  - Software strategy, process, procedure, and Documentation related to Software selection.
  - Feature requirements and objectives.
  - Upgrade planning and migration triggers, such as Software advisories, Software deferrals, Software end-of-sale (EOS), Software end-of-life (EOL), and Field Notices.

Deliverable

- Type 1 Software Management Process and Procedure Document

Type 1 Software Release Standards and Conformance

Software Release Standards and Conformance consists of the following two (2) reports described below:

- Type 1 Software Analysis and Release Standards Report
- Type 1 Software Track Conformance Report

Type 1 Software Analysis and Release Standards Report

Technologies Supported

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

Solutions Supported

- Software Defined WAN
  - Routing and Switching
- Virtual Packet Core
  - Computing Systems
  - Data Center Switching
  - Packet Core
Cisco Responsibilities

- Develop the Software Analysis and Release Standards Report, which may include:
  - Overall Software recommendation(s) that Customer should test and consider.
  - Descriptions of new Software features and Hardware compatibility.
  - Unresolved Software bugs to which Customer may be exposed and, if possible, appropriate workarounds.
  - Software feature upgrade analysis based on information gathered and analysis of findings of identified Software versions relative to Customer’s current and future Software feature requirements.

Deliverable

- Type 1 Software Analysis and Release Standards Report.
- Note: One (1) quantity of this Deliverable is for one (1) platform and its software release.

Limitation

*Specific to Data Center Orchestration and Automation
- The Type 1 Software Analysis and Release Standards Report is supported for Cisco CloudCenter only.

Type 1 Software Track Conformance Report

Technologies Supported

- Optical Networking
- Wireless Networking
- Computing Systems
- Storage Area Networking
- Data Center Switching
- Application Centric Infrastructure
- Data Center Orchestration and Automation
- Video Collaboration
- Network Security
- Cloud Security
- Security Policy and Access
- Advanced Threat
- Next Gen Cable Access
- SP Video Infrastructure
- IoT Edge and Fog Compute

Solution Supported

- Virtual Packet Core
  - Computing Systems
  - Data Center Switching

Cisco Responsibilities

- Baseline Customer’s release standards and conformance of deployed release standards against Cisco-recommended Software release standards.

Limitation

*Specific to Data Center Orchestration and Automation
- The Type 1 Software Track Conformance Report is supported for Cisco CloudCenter only.
Deliverable

- Type 1 Software Track Conformance Report

Type 1 Software Risk Management and Insights

Software Risk Management and Insights consists of the following two (2) reports described below:

- Type 1 Cisco Product Security Incident Response Team (PSIRT) Analysis and Recommendation Report
- Type 1 Software Lifecycle Milestones

Type 1 PSIRT Analysis and Recommendation Report

Technologies Supported

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

Solutions Supported

- Software Defined WAN
  - Routing and Switching
- Virtual Packet Core
  - Computing Systems
  - Data Center Switching
  - Packet Core
- SP Analytics and Assurance
  - Network Management and Orchestration

Cisco Responsibilities

- Perform the following when applicable:
  - Identify list of devices affected or potentially affected by the PSIRT.
  - Provide analysis and recommendations to address how the PSIRT may impact Customer’s existing deployed solution.
  - Provide recommended Software version where the fix for the PSIRT is incorporated.

Additional Responsibilities

*Specific to Virtual Packet Core

- This deliverable supports RedHat Openstack and RedHat Operating System (OS) software components.
Deliverable

- Type 1 PSIRT Analysis and Recommendation Report

**Type 1 Software Lifecycle Milestones**

**Technologies Supported**

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

**Solution Supported**

- Software Defined WAN
  - Routing and Switching
- Virtual Packet Core
  - Computing Systems
  - Data Center Switching

**Cisco Responsibilities**

- Perform the following when applicable:
  - Identify devices affected by Software deferral, Software EOS, and Software EOL that are applicable to Customer’s deployed Software standards and could result in a migration trigger.

Deliverable

- Type 1 Software Lifecycle Milestones Report

2.2.2b – Software Lifecycle Management, Type 2 – Cisco Cloud Hosted Analytics and Insights Portal Delivered Features

**Exclusions**

*Specific to Computing Systems*

- UCS C-Series servers not connected to Fabric Interconnect are not supported by Software Lifecycle Management, Type 2 Deliverables.

**Limitations**

*Specific to Network Security, Security Policy and Access*

- Type 2 Software Lifecycle Management features are supported only for Cisco Adaptive Security Appliance (ASA), Firepower, Firepower Threat Defense (FTD), and Identity Services Engine (ISE).
ISE is not supported for Type 2 Standard Portal Feature: Software Analysis and Release Standards and Type 2 Optional Portal Feature: Software Adoption Trends.

Software Lifecycle Management Type 2 consists of the following three (3) areas of focus:

- **Type 2 Software Management Process and Procedure Development**
- **Type 2 Software Release Standards and Conformance**
- **Type 2 Software Risk Management and Insights**

### Type 2 Software Management Process and Procedure Development

**Technologies Supported**
- Routing and Switching
- Wireless Networking
- Network Security
- Security Policy and Access

**Cisco Responsibilities**
- Collaborate with Customer to develop the Software Management Process and Procedure Document, which may include:
  - Software strategy, process, procedure, and Documentation related to Software selection.
  - Feature requirements and objectives.
  - Upgrade planning and migration triggers, such as Software advisories, Software deferrals, Software EOS, Software EOL, and Field Notices.

**Deliverable**
- Type 2 Software Management Process and Procedure Document

**Customer Responsibilities**
- Share the current practices and Documentation related to establishing, complying, and managing Software release standards and Software migration triggers.

### Type 2 Software Release Standards and Conformance

Type 2 Software Release Standards and Conformance consists of the following portal features and report described below:

- **Type 2 Standard Portal Feature: Software Analysis and Release Standards**
- **Type 2 Standard Portal Feature: Software Track Conformance**
- **Type 2 Optional Portal Feature: Software Adoption Trends**

**Type 2 Standard Portal Feature: Software Analysis and Release Standards**

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

- Virtual Packet Core
  - Computing Systems
  - Data Center Switching

Note: Platforms not supported by a portal feature are supported by the Software Analysis and Release Standards Report.

Cisco Responsibilities

- Analysis of Customer-specific tracks and deployed Software release standards.
- Overall Software recommendation(s) that Customer should test and consider.
- Descriptions of new Software features.
- Unresolved Software bugs to which Customer may be exposed and, if possible, appropriate workarounds.
- Software feature upgrade analysis of identified Software versions relative to the Customer’s current and future Software feature requirements.

Deliverable

- Type 2 Standard Portal Feature: Software Analysis and Release Standards
- Type 2 Software Analysis and Release Standards Report (if applicable)
- One (1) quantity of this Deliverable is for one (1) platform and its software release

Limitations

*Specific to Wireless Networking, Computing Systems, Storage Area Networking, Data Center Switching, Virtual Packet Core Computing Systems and Data Center Switching
- Software analysis and release standards is delivered via a report.

Type 2 Standard Portal Feature: Software Track Conformance

Technologies Supported

- Routing and Switching
- Wireless Networking
- Network Security
- Security Policy and Access

Cisco Responsibilities

- Assist Customer in creating groups of Software versions to be tracked and reported periodically through the portal.
- Baseline of Customer’s release standards and conformance of deployed release standards against Cisco-recommended Software release standards.

Deliverable

- Type 2 Standard Portal Feature: Software Track Conformance

Limitations

*Specific to Wireless Networking
• Type 2 Standard Portal Feature: Software Track Conformance feature is not available for Cisco AP-LWAN devices.

**Type 2 Optional Portal Feature: Software Adoption Trends**

**Technologies Supported**

- Routing and Switching  
- Network Security  
- Security Policy and Access

**Cisco Responsibilities**

- Software release upgrade trends observed in the Customer’s install base.

**Deliverable**

- Type 2 Optional Portal Feature: Software Adoption Trends

**Type 2 Software Risk Management and Insights**

Software Risk Management and Insights consist of the following Cisco Cloud Analytics and Insights Portal features described below:

- **Type 2 Standard Portal Feature: PSIRT Analysis and Recommendation**
- **Type 2 Standard Portal Feature: Software Lifecycle Milestones**
- **Type 2 Optional Portal Feature: Critical Bug Notification**
- **Type 2 Optional Portal Feature: Software Maintenance Update Notification**
- **Type 2 Optional Portal Feature: Software Release Bug Tracking**

**Type 2 Standard Portal Feature: PSIRT Analysis and Recommendation**

**Technologies Supported**

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

**Solution Supported**

- Virtual Packet Core
  - Computing Systems  
  - Data Center Switching

**Cisco Responsibilities**

- Cisco will perform the following when applicable:
  - Identify list of devices affected or potentially affected by PSIRT.
  - Provide analysis and recommendations to address how the PSIRT may impact Customer’s existing deployed Solution.
  - Provide recommended Software version where the fix for the PSIRT is incorporated.
**Deliverable**

- Type 2 Standard Portal Feature: PSIRT Analysis and Recommendation

**Type 2 Standard Portal Feature: Software Lifecycle Milestones**

**Technologies Supported**

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

**Solution Supported**

- Virtual Packet Core
  - Computing Systems
  - Data Center Switching

**Cisco Responsibilities**

- Identify devices affected by Software deferral, Software EOS, and Software EOL that are applicable to Customer’s deployed Software standards and could result in a migration trigger.

**Deliverable**

- Type 2 Standard Portal Feature: Software Lifecycle Milestones

**Type 2 Optional Portal Feature: Critical Bug Notification**

**Technology Supported**

- Routing and Switching
- Network Security
- Security Policy and Access

**Cisco Responsibilities**

- Provide Critical Bug Notification alerting the Customer of discovery, status change, or resolution of critical bugs in preferred Software release tracks.

**Deliverable**

- Type 2 Optional Portal Feature: Critical Bug Notification
- One (1) quantity of this Deliverable is for one (1) platform and its software release.

**Type 2 Optional Portal Feature: Software Maintenance Update Notification**

**Technology Supported**

- Routing and Switching
Cisco Responsibilities

- Provide Software Maintenance Update Notification alerting the Customer of the availability of a patch or maintenance Update for a specific bug, feature, or Software release.

Deliverable

- Type 2 Optional Portal Feature: Software Maintenance Update Notification
- One (1) quantity of this Deliverable is for one (1) platform and its software release.

Type 2 Optional Portal Feature: Software Release Bug Tracking

Technology Supported

- Routing and Switching
- Security Policy and Access
- Network Security

Cisco Responsibilities

- Provide periodic insights and tracking of critical bugs for specified Software release standards.

Deliverable

- Type 2 Optional Portal Feature: Software Release Bug Tracking

2.2.2c – Software Lifecycle Management, Type 3 – Cisco OnPrem Analytics and Insights

Tool-Delivered Reports

Limitations

*Specific to Network Security, Security Policy and Access

- Type 3 Software Lifecycle Management reports are supported only for Cisco Adaptive Security Appliance (ASA), Firepower, Firepower Threat Defense (FTD), and Identity Services Engine (ISE).

Software Lifecycle Management Type 3 is provided via Cisco OnPrem Analytics Tool, and consists of the following three (3) areas of focus:

- Type 3 Software Management Process and Procedure Development
- Type 3 Software Release Standards and Conformance
- Type 3 Software Risk Management and Insights

Type 3 Software Management Process and Procedure Development

Technology Supported

- Routing and Switching
- Security Policy and Access
- Network Security

Cisco Responsibilities

- Collaborate with the Customer to develop the Software Management Process and Procedure Document, which may include:
Main: **Foundation Theme**  |  Section Navigation: **Compliance and Remediation**

- Software strategy, process, procedure, and Documentation related to Software selection.
- Feature requirements and objectives.
- Upgrade planning and migration triggers, such as Software advisories, Software deferrals, Software EOS, Software EOL, and Field Notices.

**Deliverable**

- Type 3 Software Management Process and Procedure Document

**Type 3 Software Release Standards and Conformance**

**Technology Supported**

- Routing and Switching
- Data Center Switching
- Network Security
- Security Policy and Access

**Cisco Responsibilities**

- Baseline Customer’s release standards and conformance of deployed release standards against Cisco-recommended Software release standards.
- Develop the Software Analysis and Release Standards, which may include:
  - Overall Software recommendation(s) that Customer should test and consider.
  - Descriptions of new Software features and Hardware compatibility.
  - Unresolved Software bugs to which Customer may be exposed and, if possible, appropriate workarounds.
  - Software feature upgrade analysis based on information gathered and analysis of findings of identified Software versions relative to Customer’s current and future Software feature requirements.

**Deliverables**

- Type 3 Software Track Conformance Report
- Type 3 Software Analysis and Release Standards Report
- Note: One (1) quantity of Type 3 Software Analysis and Release Standards Report is for one (1) platform and its software release.

**Type 3 Software Risk Management and Insights**

**Technology Supported**

- Routing and Switching
- Data Center Switching
- Network Security
- Security Policy and Access

**Cisco Responsibilities**

- Perform the following when applicable:
  - Identify list of devices affected or potentially affected by PSIRT.
  - Provide analysis and recommendations to address how the PSIRT may impact Customer’s existing deployed solution.
  - Provide recommended Software version where the fix for the PSIRT is incorporated.
Devices affected by Software deferral, Software EOS, and Software EOL that are applicable to Customer’s deployed Software standards and could result in a migration trigger.

Deliverables
- Type 3 PSIRT Analysis and Recommendation Report
- Type 3 Software Lifecycle Milestones Report

2.2.3 – SOFTWARE COMPLIANCE AND REMEDIATION

Software Compliance and Remediation provides an automated way to help identify Network devices that are out of Software compliance, and guides the Customer through the steps to remediate / upgrade to the required OS version based on current and deployed recommended releases outlined in Software Analysis and Release Standards Report and Software Track Conformance Report.

Software Compliance assesses the state of the Network’s OS based on a certain standard or guideline (in this case, the Software Analysis and Release Standards Document). The details of the vendor, Product, and OS support for this Service are below.

The script provides Software upgrades for a single device or large groups of devices by utilizing the MOP Document and the pre-check and post-check document 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:**
  - Cisco Software Analysis and Release Standards Report
  - Cisco Software Track Conformance Report

- **Configuration and Software Change Support:**
  - Cisco Change Implementation Review and Recommendation Report

Technology 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.

Additional Information to be Collected

- Customer’s completed Cisco Software Track Conformance Report.

Cisco Responsibilities

- Create upgrade automation rules and conditions for one (1) Platform / Operating System.
Main: Foundation Theme | Section Navigation: Compliance and Remediation

- 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 Cisco Software Analysis and Release Standards Report, a prerequisite for this Deliverable.
- Complete Cisco Software Track Conformance Report, a prerequisite for this Deliverable.
- Complete Cisco Change Implementation Review and Recommendation Report, a prerequisite for this Deliverable.

### 2.2.4 – Configuration Compliance and Remediation

Configuration Compliance and Remediation provides the Customer with an automated way to identify Network devices that are out of configuration compliance, and guides them through the steps to remediate / upgrade to the required standard based on recommendations outlined in the Platform Insights - Configuration Best-Practices Report and/or Policy Configuration Report.

The Configuration Compliance Deliverable provides remediation for the target Network devices using scripts based on the procedures, pre-conditions, and success criteria outlined in the Configuration Best-Practices Report and the Policy Configuration Conformance Document.

**Dependency**

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

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

**Technology Supported**

- Routing and Switching
- Network Security
- Wireless Networking

**Note:** [Cisco Business Critical Services General Terms - Cisco General Responsibilities - Limitations](#) contains the 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.
- Remediate the Platforms / Operating systems to the recommended best-practices policy outlined in the Cisco Best-Practices Report.
- Provide successful job log reports.

Deliverable

- One (1) configuration compliance script per Platform / Operating System specified in the Quote.

Customer Responsibilities

- Complete Cisco Configuration Best-Practices Report, a prerequisite for this Deliverable.
- Complete Cisco Policy Configuration Conformance Report, a prerequisite for this Deliverable.
- Complete Cisco Change Implementation Review and Recommendation Report, a prerequisite for this Deliverable.

2.2.5 – Regulatory Compliance and Remediation

The Regulatory Compliance and Remediation provides Customers with an automated way to assist Customer in identifying Network devices that are out of configuration compliance in the context of industry standards (listed below), and guides the Customer through the steps to assist Customer to remediate based on those standards.

Network Configurations are audited against rules in various categories like Routing, Switching, and Security within these standards body regulations, and results are provided per-device and aggregated.

Customers will be able to review the results of the audit to help plan maintenance windows based on their prioritization of the exceptions and Network devices, and execute Customer’s remediation plan. The dashboard views provide a level of detail for Network engineering staff, operations teams, auditors, and executives to view the results and 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 regulatory and legal compliance requirements associated with the industry standards identified in this Service. Cisco will provide assessments and recommendations based on Cisco practices and will perform remediation tasks per Customer instruction.

Dependency

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

Usage

Cisco Security Compliance Assessment Deliverable: Customers purchase a Security Compliance Assessment for one or more standards such as HIPAA, ISO 27002, PCI DSS, DISA DoD STIG, and other standard regulatory requirements, if available. The compliance assessment assists Customer to
determine current adherence to the above security standards, identify gaps, and provide
recommendations on how to remediate those gaps.

The Regulatory Compliance and Remediation Deliverable is intended for:

- Customers who want to take the results from a Cisco Security Compliance Assessments Deliverable
  and implement them in the Network based on the scope outlined below, OR
- 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.

**Technology 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**

- Enable the following Regulatory Conformance Assessments via the Cisco NCCM Software:
  - 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 Regulatory Conformance Assessment 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 Regulatory Conformance Assessment.
- Provide job log reports.

**Additional Responsibilities**

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

- 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 vulnerability assessment.
Deliverables

- One (1) regulatory conformance configuration assessment report.
- One (1) regulatory configuration compliance script per Cisco Platform / Operating System 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
3—OPERATIONAL PROFICIENCY

Operational Proficiency provides analysis and recommendations for improvements to the maturity of operational process, measurement, tooling capabilities, and resources that help increase skills and knowledge of Cisco technologies.

SECTION NAVIGATION

Foundation Theme – Operational Proficiency includes the following Service capabilities and Deliverables:

- **3.1 – Instrumentation Management**
  - 3.1.1 – Management Instrumentation Review
  - 3.1.2 – Management Deployment Planning and Readiness Assessment

- **3.2 – Metrics Management**
  - 3.2.1 – KPI Definition, Implementation, and Report
  - 3.2.2 – KPI Audit and Recommendations
  - 3.2.3 – KPI Trending and Reporting
  - 3.2.4 – Mapping Operational Metrics to Business Outcomes
  - 3.2.5 – Security Metrics Program Development

- **3.3 – Operations Management**
  - 3.3.1 – Operations Risk Management Assessment
  - 3.3.2 – Operations Risk Remediation
  - 3.3.3 – Operations Process or Run Book Update
  - 3.3.4 – IT Operations Model Analysis
  - 3.3.5 – Escalation Engineering Support
  - 3.3.6 – Asset Management
  - 3.3.7 – Incident Management
  - 3.3.8 – Problem Management
    - 3.3.8a – Problem Management – High-Touch Technical Support
    - 3.3.8b – Problem Management – High-Touch Engineering
  - 3.3.9 – Asset Management
  - 3.3.10 – Incident Management
  - 3.3.11 – Problem Management
  - 3.3.12 – Problem Management – High-Touch Engineering

- **3.4 – Knowledge Management**
  - 3.4.1 – Knowledge Transfer Session
  - 3.4.2 – Specialized Knowledge Session
  - 3.4.3 – Cyber Range Workshop
  - 3.4.4 – Learning Library
    - 3.4.4a – Technical Knowledge Library
    - 3.4.4b – Cisco Platinum Learning Library
  - 3.4.5 – Cisco Training
    - 3.4.5a – Cisco Open Enrollment Training
    - 3.4.5b – Cisco Closed Enrollment Private Group Training

- **3.5 – Classified Network**
  - 3.5.1a – CNS High-Touch Operations Management
  - 3.5.1b – CNS High-Touch Technical Support
3.1 – Instrumentation Management

Instrumentation Management analyzes management goals against current capabilities and features, assesses impact of new requirements, and provides recommendations to align management solution design with priorities, goals, and objectives.

3.1.1 – MANAGEMENT INSTRUMENTATION REVIEW

Management Instrumentation Review assists Customer’s operations staff to achieve current and future Network Management business and operational objectives by incorporating Cisco’s architecture and operational best practices.

Cisco Engineers assess Customer’s Solution architecture and technical design requirements (capability, resiliency, efficiency, scaling), perform a current-state capability and risk assessment, and provide recommendations to help Customer achieve business and operational objectives. Cisco optimizes visibility and control of Customer’s IT environment for one (1) architecture.

Technologies Supported

- Network Management and Orchestration

Solution Supported

- Software Defined WAN
  - Network Management and Orchestration

Cisco Responsibilities

- Analyze Customer’s requirements, current practices, and capabilities compared to Cisco-recommended best practices.
- Analyze impact of new requirements on existing Network Management infrastructure and operations support.
- Provide assistance in aligning Management Instrumentation design with Network architecture evolution.
- Update current Network Management Instrumentation design Documentation.

Additional Responsibilities

*Specific to Network Management and Orchestration

- Review and provide recommendations for the following:
  - Management protocol selection and configuration
  - Feature selection and configuration of existing Network Management Instrumentation applications
  - Security considerations
Deliverable

- Management Instrumentation Review Report

3.1.2 – MANAGEMENT DEPLOYMENT PLANNING AND READINESS ASSESSMENT

The Management Deployment Planning and Readiness Assessment Service assists Customer’s Operations staff to prepare for management Software Solution post-implementation maintenance. Cisco validates Customer implementation plans and processes, reviews test cases and results, and advises on impact to operational processes.

Technologies Supported

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

Solutions Supported

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

Cisco Responsibilities

- Validate Customer solution implementation plans and processes.
- Validate Customer solution test objectives, plans, results, and issues.
- Advise Customer on recommended improvements to address operational process capabilities and readiness.

Deliverable

- Consultative guidance and support only

3.2 – Metrics Management

Metrics Management assists with reviewing measurement goals and requirements; evaluates effectiveness of current metrics against recommended metrics and tooling capabilities; and helps with steps to define, align, measure, and report on KPIs to improve visibility and decision-making.

3.2.1 – KPI DEFINITION, IMPLEMENTATION, AND REPORT

The KPI Definition, Implementation, and Report Service provides assistance to define and establish a framework for measuring Cisco Management Software Solution and system Critical Success Factors (CSF) and KPIs. The scope of KPIs can include functional KPIs, such as Service provisioning, fault, performance, and configuration management, as well as system performance KPIs including memory, processing, and database capacity.
Technologies Supported
- Network Management and Orchestration
- Data Center Orchestration and Automation

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

Exclusion
*Specific to Data Center Orchestration and Automation
- Cisco CloudCenter (CCC) is not supported.

Cisco Responsibilities
- Evaluate potential Customer-required KPIs based on Cisco-recommended KPIs.
- Define KPI data collection sources, process, automation opportunities, and target thresholds.
- Define KPI functional ownership, process ownership, and review frequency.

Deliverable
- KPI Framework Report

Customer Responsibilities
- Provide CSF and KPI requirements and priorities.

3.2.2 – KPI AUDIT AND RECOMMENDATION

KPI Audit and Recommendation collects and analyzes KPIs from the Cisco Solution over a specified timeframe, and looks for issues in the areas of Fault, Performance, Capacity, and Configuration Management that relate directly to the stability and availability of Customer’s solution. Quote for Services will specify the Cisco Solution(s) supported.

Solutions Supported
- Cisco Policy Solution (CPS), Self-Optimizing Network (SON)
  - Mobility Policy and Access
- SP Analytics and Assurance
  - Network Management and Orchestration

Cisco Responsibilities
- Create the KPI Audit and Recommendations Report:
  - For Cisco Policy Solution (CPS):
    - If applicable, the following KPIs on both Gx and Gy interface will be part of the report:
      - Credit Control Request – Success, dropped, and error rate.
      - Reauthorization request – Success, dropped, and authorization rate.
    - If applicable, the following KPIs on Sy interface will be part of the report:
Main: Foundation Theme | Section Navigation: Operational Proficiency

- Spending Limit Request – Success rate.
- Spending Status Notification – Success rate.
- Session Termination Request – Success rate.
  
  - For Cisco SON Solution:
    - Top Offender Analysis and Recommendations:
      - Generate monthly reports for top offenders with highest drop-call rate (DCR).
      - Optimize SON settings for these offenders to get KPI improvements.
      - Recommend preliminary solutions for top offenders.
    - SON Reports: KPI / Boomer Report:
      - Boomer and Primary Scrambling Code (PSC) collision reports will be provided based on Customer’s request.
      - Activity Report for application to show SON actions.
      - KPI metrics for Remote Network Controllers (RNC) and Network level.
      - Count of new cell neighbor activity by SON.

**Deliverable:**

- KPI Audit and Recommendations Report

### 3.2.3 – KPI TRENDING AND REPORTING

KPI Trending and Reporting provides regular analysis of Cisco Management Software Solution, process, system KPIs trends and deviations from the baseline, and recommendations for improvement. Scheduled Service is performed at a frequency agreed with the Customer (recommended once every quarter).

**Technologies Supported**

- Network Management and Orchestration
- Data Center Orchestration and Automation

**Solutions Supported**

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

**Exclusion**

*Specific to Data Center Orchestration and Automation*

- Cisco CloudCenter (CCC) is not supported.

**Cisco Responsibilities**

- Analyze Customer KPI performance trends to identify deviations from baseline targets.
- Evaluate multiple viewpoints such as design, capacity, support, and operations.

**Deliverable**

- KPI Evaluation Report
3.2.4 – MAPPING OPERATIONAL METRICS TO BUSINESS OUTCOMES

Mapping Operational Metrics to Business Outcomes aligns Customer’s desired business outcomes to relevant operational metrics and provides recommendations for how those metrics can be measured, together with identifying appropriate operational tooling.

**Technologies Supported**
- Application Centric Infrastructure
- Computing Systems

**Solution Supported**
- SP Analytics and Assurance
  - Network Management and Orchestration

**Cisco Responsibilities**
- Determine a ranked list of business outcomes and IT Services provided by the IT Infrastructure.
- Determine IT operational metrics that can be used to measure the degree to which business outcomes are being achieved.
- Determine operational tooling that Customer can consider to optimize the collection and reporting of selected metrics.

**Deliverable**
- Presentation of IT Operational Metrics and Operational Tooling aligned with Business Outcomes

**Customer Responsibilities**
- Agree to pilot measurement and reporting of one or more agreed-upon operational metrics.

3.2.5 – SECURITY METRICS PROGRAM DEVELOPMENT

Cisco will assist Customer in developing a Security Metrics Program, including analysis and creation of an initial security metrics catalog and dashboards based on Customer needs and requirements.

Cisco will leverage recognized standards for security measurement and metrics, including ISO 27004: Information Technology – Security Techniques – Information Security Management – Measurement. Cisco uses a combination of approaches to deliver a Security Metrics Program Development engagement, including educational workshops, individual and group working sessions, and review of artifacts. The resulting Deliverable will include recommendations for strategic and tactical improvement of the measurement program, as well as specific metrics and dashboards developed over the course of delivery.

**Architecture Supported**
- Security
Cisco Responsibilities

- Review the maturity of the Customer’s current IT and Information Security Measurement Program.
- Facilitate an introductory Security Metrics Workshop with business and technical resources to:
  - Provide an overview of measurement in industry.
  - Provide an overview of specific measurement applications in information and IT security.
  - Provide an overview of ISO 27004 and other appropriate security measurement standards and frameworks.
  - Explain the Goal-Question-Metric (GQM) methodology.
  - Discuss specific security measurement examples and case studies.
  - Discuss and identify key security questions and metrics that need to be answered and reported on a regular basis.
- Analyze workshop results and applicability to the overall engagement.
- Compare existing program to recommendations and requirements of ISO 27004 and other measurement frameworks.
- Facilitate GQM workshops with business and technical resources for purposes of developing and improving the Customer’s metrics catalog, which may include the following activities:
  - Use GQM techniques to define and explore specific strategic measurement scenarios for new or existing Customer security metrics.
  - Analyze GQM results, and incorporate them into the metrics catalog.
- Provide recommendations for executive and management dashboards as well as a roadmap for metrics maturity.

Deliverable

- Security Metrics Recommendation Report

3.3 – Operations Management

Operations Management assesses operations model, processes, and tooling capabilities for improvements to operational practices and maturity, and assists with steps to evaluate and remediate risk of operational gaps. Cisco and Customer will collaborate with Cisco Technical Assistance Center (TAC) and appropriate business units for open Cisco Priority 1 (P1) and Priority 2 (P2) cases.

3.3.1 – OPERATIONS RISK MANAGEMENT ASSESSMENT

Operations Risk Management Assessment reviews Customer’s ITSM operational processes and tools that support the processes, and provides recommendations for improvements to operational practices to optimize operations of Cisco technology for one (1) architecture.

Technologies Supported

- Routing and Switching
- Computing Systems
- Storage Area Networking
- Data Center Switching
- Application Centric Infrastructure
Cisco Responsibilities

- Determine the focus for the assessment, which may include Event, Incident, Problem, Knowledge, Service Asset and Configuration, Change, Service Catalog, Performance, and Capacity Management.
- Analyze Customer’s current process effectiveness in maximizing Service availability.
- Correlate Customer’s processes with Cisco best practices.
- Determine changes to operations processes for optimizing the operations of Cisco technology for service availability.

Deliverable

- Operations Risk Management Assessment Presentation

3.3.2 – OPERATIONS RISK REMEDIATION

Operations Risk Remediation provides Remote access to Cisco IT Service Management (ITSM) Subject Matter Expert Consultant to supplement Customer personnel.

Technologies Supported

- Routing and Switching
- Wireless Networking
- Computing Systems
- Storage Area Networking
- Data Center Switching
- Application Centric Infrastructure
- SP Video Infrastructure
- IoT Edge and Fog Compute

Cisco Responsibilities

- Use Customer-provided data, scripts, or internal process and tools Documentation to assist in providing consulting support, as needed.
- Provide targeted consulting support as directed by Customer during Customer’s normal business hours.
- Identify Deliverables necessary for Service transition to Customer’s operations team.
- Provide consultant skillset and role, which may include:
  - Plan, design, and/or lead the development of ITSM processes identified above.
  - Facilitate standardization and adoption of ITSM processes within Customer operations organization.
  - Serve as an advisor to Customer in regards to operations excellence and/or operations transformation.
  - Provide Cisco and industry best practices to Customer regarding infrastructure and/or IT Service operations, including comparison against other industry operations maturity benchmarks.
  - Articulate “as a Service” industry practices.
  - Provide an understanding of multiple ITSM and development methodologies, which may include eTOM, COBIT, TOGAF, and DevOps, as well as ITIL.

Deliverable

- Consultative guidance and support only
Customer Responsibilities

- Request direct Cisco consulting support in the areas of ITSM process, tools design, and implementation support.
- Provide targeted areas in which ITSM consultancy is required.

3.3.3 – OPERATIONS PROCESS OR RUN BOOK UPDATE

Operations Process or Run Book Update assists in updating an existing Operational Run Book or Standard Operating Procedure (SOP) that addresses a specific operational or technical function for a one (1) Product technical Solution or IT Service.

Technologies Supported

- Wireless Networking
- Computing Systems
- Storage Area Networking
- Data Center Switching
- Application Centric Infrastructure

Cisco Responsibilities

- Update Run Book or SOP consistent with Cisco best practices.

Deliverable

- Updated Run Book or SOP

3.3.4 – IT OPERATIONS MODEL ANALYSIS

IT Operations Model Analysis provides an accelerated assessment to determine key operational issues associated with critical operational functions applied to one (1) architecture, identifying which next steps would be most beneficial to mitigate operational risk. Area of focus may be determined or triggered by an unexpected operational event.

Technologies Supported

- Routing and Switching
- Computing Systems
- Storage Area Networking
- Data Center Switching
- Application Centric Infrastructure

Cisco Responsibilities

- Perform an assessment focused on one (1) architecture and one or more ITSM processes to identify key operational issues.

Deliverable

- IT Operations Model Presentation
3.3.5 – Escalation Engineering Support

Escalation Engineering Support enhances the Customer’s Incident and Problem Management process by providing assistance with Cisco TAC restoration of Service activities for unplanned or unscheduled incidents.

**Technologies Supported**

- Routing and Switching
- Wireless Networking
- Network Management and Orchestration
- Data Center Orchestration and Automation
- Tetration
- Unified Communications
- Customer Care
- Video Collaboration
- Cloud Meetings and Messaging
- Network Security
- Cloud Security
- Security Policy and Access
- Advanced Threat
- Packet Core
- Next Gen Cable Access
- IoT Edge and Fog Compute

**Solutions Supported**

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

**Cisco Responsibilities**

- Perform technical evaluation with Cisco TAC escalation after following the proper Cisco TAC procedures, diagnosis, and escalation process.
- Collaborate with Cisco TAC regarding Customer’s Cisco environment to assist Cisco TAC and the appropriate Cisco business unit(s) in resolving the incident.
- Assist Customer with Remote support in dealing with open P1 and P2 cases.
- Assist Customer in analyzing recurring problem(s) and root cause(s), including providing consultative support for development of a plan of action to prevent, address, and minimize the business impact of the problem(s).

**Additional Responsibilities**

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

- Cisco Project Manager will assign an Engineer to remotely track and help with the resolution of the issue(s) related to the Cisco Collaboration Solution for P1 and P2 cases only.

**Deliverable**

- Consultative guidance and support only
Customer Responsibilities

- Provide Cisco access to users that have been contacting the Customer’s support desk or resolution center for assistance in connection with the Cisco components or Service problems or issues.
- Notify Cisco Services of the open ticket needing assistance, and provide Cisco TAC case number.

Note: Customer shall not escalate any related problems or issues until Cisco TAC has performed diagnostics.
- Work with Cisco TAC on the resolution and closure of problem / case, and involve Cisco Network Consulting Engineer only on critical P1 and P2 cases, as needed.

Limitations

- The following are not provided or a part of the Escalation Engineering Support Service:
  - Cisco Services Engineer does not make any changes to the Customer Production environment.
  - The Service does not cover P3 / P4 Cisco TAC cases.
  - There must be an onsite presence for Cisco TAC case support.
- This Deliverable does not replace Cisco TAC, Cisco High-Touch Operations Management, Cisco High-Touch Technical Support, or any other form of technical Services and support, including Third-Party Support.
- Cisco Technical Services, Cisco TAC, and any of the following Services Customer may have, such as High-Touch Technical Support, High-Touch Operations Management, and Focal Engineer, are responsible for case escalation, resolution, and engaging and involving appropriate resources like Cisco business unit(s) and third-party vendors, as well as for providing any and all status updates and communications related to the case and case closure.

3.3.6 – ASSET MANAGEMENT

Asset Management provides Customer with Cisco best practices for managing assets and contracts based on the Customer inventory, reporting of asset moves, adds, changes and deletions (MACD), and monitoring of asset coverage and entitlement.

Solution Supported

- High-Touch Expert Care

Additional Information to be Collected

- Customer’s record of inventory and service contract details.
- Customer’s record of serial number removed and replaced by Return Material Authorization (RMAs).

Cisco Responsibilities

- Provide reporting on the Customer’s inventory which may include the following:
  - Changes to address inventory Service coverage, co-termination, and location.
- Provide documented process for IT asset moves, adds, changes and deletions.

Deliverables

- MACD Best Practices Report
**3.3.7 – INCIDENT MANAGEMENT**

Incident Management provides a single point of contact, a Cisco High-Touch Operations Manager ("HTOM"), for the management of all incidents. The HTOM has knowledge of the Customer processes, Cisco support organizations, escalation process and coordinates to help restore Customer service operations. For Onsite Incident Management this Deliverable must be purchased with Foundation Onsite Support Deliverable.

**Note:** Service Monitoring and Reporting Deliverable is provided with Incident Management.

**Solution Supported**

- High-Touch Expert Care

**Additional Information to be Collected**

- Customer’s Network Operations Center (NOC) setup such as staffing groups, tools, communications and escalation process, contacts, field support groups.

**Cisco Responsibilities**

- Facilitate problem resolution on a reactive basis for technical issues reported to Cisco by Customer.
- Provide twenty-four (24) hours a day, seven (7) days a week incident management for case request and escalation management support for Severity 1 and Severity 2 cases during non-Standard Business Hours.
- Follow-ups within Cisco and Customer, and identify Service Request response gaps.
- Coordinate Cisco support organizations, escalation process, and Customer resources for Service Requests.
- Conduct post incident review to determine recommendations for corrective actions and best practices for improving operational support processes.
- Conduct operational assessment of Customer’s current processes and recommend best practices for incident and event management.

**Deliverable**

- Facilitate incident and problem resolution
3.3.8 - PROBLEM MANAGEMENT

Problem Management provides access to Cisco High-Touch Technical Support or Cisco High-Touch Engineering familiar with your networking environment.

3.3.8a – Problem Management - High-Touch Technical Support

Provides twenty-four (24) hours a day, seven (7) days a week direct access to a Cisco High-Touch Technical Support (“HTTS”) team of specialists. The HTTS team helps troubleshoot your Cisco network for complex and critical issues, and provides remediation support to help resolve identified issues. HTTS provides two support options: a pooled High-Touch Technical Support team, or Dedicated High-Touch Technical Support team.

Dependency

- Incident Management Service is required.

Additional Information to be Collected

- Customer’s proposed current and planned hardware changes, software upgrades and or configuration changes, methods of procedures (MOP).

Solution Supported

- High-Touch Expert Care

Cisco Responsibilities

- Provide case tracking and troubleshooting which includes the following:
  - Provide direct access where available, twenty-four (24) hours per day, seven (7) days per week basis to a HTTS team via a Cisco provided contact information.
  - Provide proactive maintenance window support which includes the following:
    - Work with the Customer to create a Service Request for a scheduled maintenance window.
    - Provide recommended changes to Customer’s implementation plan, MOP, and test plan based on information gathered from the Customer.
    - Provide remote standby support during scheduled maintenance window.

Note: The Cisco High-Touch Expert Care Service Level Agreement terms and conditions for Response Time and Restoration Time is documented in the Cisco Business Critical Services General Terms Section 5 - Cisco High-Touch Expert Care Service Level Agreement.

Limitations

- Cisco is not responsible for testing any procedures in support of Customer’s proposed or planned changes.
- Cisco is not responsible for developing MOPs.
Deliverables

- Case Tracking and Troubleshooting
- Proactive Maintenance Window Support

Note: The Quote will specify pooled or dedicated High-Touch Technical Support.

3.3.8b – Problem Management - High-Touch Engineering

Provides direct access to a Cisco High-Touch Engineer (“HTE”), which has both technical knowledge and familiarity with your networking environment. High-Touch Engineer helps troubleshoot your Cisco network for complex and critical issues, and provides remediation support to help resolve identified issues. For Onsite Problem Management – High Touch Engineering this Deliverable must be purchased with Foundation Onsite Support Service.

Dependency

- Incident Management Deliverable is required with this Service.
- Performance of a root cause analysis by Cisco is dependent upon all the necessary information available to Cisco in a timely manner.

Additional Information to be Collected

- Customer’s proposed current and planned hardware changes, software upgrades and or configuration changes, methods of procedures (MOP).

Solution Supported

- High-Touch Expert Care

Cisco Responsibilities

- Provide case tracking and troubleshooting which includes the following:
  - Provide direct access where available, during Standard Business Hours, to the HTE via a Cisco provided contact information.
  - Perform root cause analysis on high severity technical issues in the Network Infrastructure.
- Provide proactive maintenance window support which includes the following:
  - Work with the Customer to create a Service Request for a scheduled maintenance window.
  - Provide recommended changes to Customer’s implementation plan, MOP, and test plan based on information gathered from the Customer.
  - Provide remote standby support during scheduled maintenance window.

Deliverables

- Root Cause Analysis Report
- Problem Management
- Proactive Maintenance Window Support
3.4 – Knowledge Management

Knowledge Management assists Customer’s efforts to enhance technical knowledge and skills such as knowledge transfer sessions, access to technical knowledge library, and specialized technical training workshops.

3.4.1 – KNOWLEDGE TRANSFER SESSION

Knowledge Transfer Session provides technical information transfer on topics mutually agreeable and relevant to the Cisco Products and technologies deployed in the Customer’s environment. Sessions focus on best practices for operating, tuning, troubleshooting, maintaining, and managing Cisco Solutions deployed. 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
- Software Defined WAN
  - Routing and Switching
  - Network Management and Orchestration

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 (OS) 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.
- Understand that the Knowledge Transfer Sessions will be performed remotely; if scheduled at a Customer site, Customer will be responsible for any additional costs.
- 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.

3.4.2 – SPECIALIZED KNOWLEDGE SESSION

Specialized Knowledge Session is a structured information transfer with hands-on labs (if applicable) on pre-defined topics relevant to the Cisco Products and technologies deployed in the Customer’s environment. Sessions focus on Cisco best practices for operating, tuning, troubleshooting and maintaining Cisco Solutions deployed. Specialized Knowledge Sessions are not a replacement for any authorized Cisco Education or Learning@Cisco classes.

3.4.2a – Specialized Knowledge Session

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

3.4.2b – Specialized Knowledge Session

Technology 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:
  - CloudCenter Overview:
    - One (1) day duration, delivered remotely.
  - CloudCenter Application and Services Modeling:
    - Three (3) days duration, delivered remotely with hands-on lab.
  - 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.

3.4.3 – CYBER RANGE WORKSHOP

Security Cyber Range provides a specialized technical training workshop to help Customer’s security staff build the skills and experience necessary to help combat modern cyberthreats.

Architecture Supported

- Security

Cisco Responsibilities

- Provide Customer workshop requirements and agenda.
- Provide standard Cyber Range workshop environment housed at a Cisco lab via remote VPN.

Deliverables

- Workshop materials, as applicable
- Workshop Attendance Certificate (if earned)
- Service Completion Certificate (if earned)

Customer Responsibilities

- Assume responsibility for the management, support, and direction of the resource supplied to Customer by Cisco.
- Provide Cisco with a connection to the Internet to access the Cyber Range workshop environment housed at a Cisco lab if the workshop is conducted at Customer site.
- Confirm workshop requirements are fulfilled two (2) weeks prior to workshop.
- Provide list of up to twelve (12) workshop attendee names.
- Attend Cyber Range Workshop at scheduled times.

Limitations

- Workshops are limited to twelve (12) attendees.
- Workshops are limited to three (3) days to five (5) days on site at a single Cisco-approved Customer location during Standard Business Hours, excluding Cisco holidays, locally recognized country holidays, vacations, and training days; or, if both Customer and Cisco agree, the workshop may be held at a designated Cisco location.

3.4.4 – LEARNING LIBRARY

Learning Library provides access to Cisco Services leading best practices, case studies, books from Cisco press, on-demand technical assets, on-line courses and interactive hands-on labs.
The following two libraries are available:

- Technical Knowledge Library
- Platinum Learning Library

### 3.4.4a – Technical Knowledge Library

Technical Knowledge Library (TKL) is a subscription-based Service that provides access to Cisco Services best practices and technical knowledge developed by Cisco Services Engineers. The library provides end-users with access to learning resources and technical information such as whitepapers, design and implementation guides, case studies, books from Cisco press, live webinars, and videos-on-demand. The library is made available by Cisco through a secure, web-based portal.

TKL is only available to certain geographic locations and will be specified in the Quote.

#### Technologies Supported
- Routing and Switching
- Wireless Networking
- Computing Systems
- Storage Area Networking
- Data Center Switching
- 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

#### Solution Supported
- Virtual Packet Core
  - Packet Core

#### Cisco Responsibilities
- Make content available to the specified number of authorized viewers in the Customer’s Quote, including multimedia clips in the form of video-on-demand or audio-on-demand content, as well as sidebar content such as whitepapers, case studies, design guides, configuration guides, troubleshooting guides, training documents, deployment guides, online textbooks and/or manuals, or bumper clips.
- Provide list of web-based trainings delivered via the portal to authorized viewers.

**Note:** Cisco may revise, Update, and/or remove previously released multimedia clips and/or sidebar content (Updated Content). Cisco will make any Updated Content available to Customer as a part of the Services. The Updated Content will exclude the previously released multimedia clips and sidebar content (where applicable) that the Updated Content was intended to supersede.

#### Deliverable
- Access to TKL, an online library of learning resources and technical information
3.4.4b – Cisco Platinum Learning Library

The Cisco Platinum Learning Library (CPLL) consists of a collection of on-demand technical assets, on-line courses and interactive hands-on labs. A Cisco Learning Advisor assists the Customer with curriculum recommendations and CPLL course consumption.

Solution Supported

- High-Touch Expert Care

Cisco Responsibilities

- Access to a Cisco Learning Advisor, who will assist with curriculum recommendations and CPLL course consumption
- Provide access to CPLL on-demand technical assets, on-line courses and interactive hands-on labs.

Deliverable

- Access to Cisco Platinum Learning Library

Note: Number of seats to access the CPLL will be specified in the quote.

3.4.5 – CISCO TRAINING

Cisco Training provides access to a catalog of more than 250 different courses on certification and product training available for open and closed (private group) enrollment. A Cisco Learning Advisor assists the Customer with course selection and scheduling.

3.4.5a – Cisco Open Enrollment Training

Cisco Open Enrollment Training provides access to a catalog of instructor-led certification and product training courses, available for open enrollment to the public. Training is delivered at Cisco training facilities or at Cisco Authorized Learning Partners. A Cisco Learning Advisor assists the Customer with course selection and scheduling.

Solution Supported

- High-Touch Expert Care

Cisco Responsibilities

- Seats in publicly offered classes from a catalog of instructor-led certification and product training courses. Classes are delivered live or virtually.

Deliverable

- Seats in Cisco Open Enrollment Training

Customer Responsibilities

- At least forty-five (45) days in advance of a course provide a list of participants, their role and function as it relates to the focus of the course.
Coordinate and schedule Cisco Training with a Cisco Learning Advisor.

### 3.4.5b – Cisco Closed Enrollment Private Group Training

Cisco Closed Enrollment Private Group Training provides access to a catalog of instructor-led certification and product training courses, available for a private group of up to twelve (12) people. Training is delivered at the Customer’s location and tailored to their network. A Cisco Learning Advisor assists the Customer with course selection and scheduling.

**Solution Supported**
- High-Touch Expert Care

**Cisco Responsibilities**
- Seats in private group training classes from a catalog of instructor-led certification and product training courses. Classes are delivered live or virtually.

**Deliverable**
- Seats in Cisco Closed Enrollment Private Group Training

**Customer Responsibilities**
- At least forty-five (45) days in advance of a course provide a list of participants, their role and function as it relates to the focus of the course.
- Coordinate and schedule Cisco Training with a Cisco Learning Advisor.

### 3.5 – Classified Network (U.S. Only)

Classified Network provides Deliverables which assist the Customer with Services for supporting Classified Network.

#### 3.5.1 - CLASSIFIED NETWORK SUPPORT

Cisco Classified Network Support (CNS) assists the Customer with facilitating timely problem resolution of issues reported to Cisco. Customers are provided reactive, direct, around the clock support by cleared support engineers familiar with Customer’s Network design and operations. CNS delivers advanced technical troubleshooting using a pool of certified experts on a wide variety of technologies and Cisco solutions.

Classified Network Support consists of the following components:
- CNS High-Touch Operations Management
- CNS High-Touch Technical Support
3.5.1a – CNS High-Touch Operations Management (U.S. Only)

Note: CNS High-Touch Operations Management Deliverable is purchased using a single Cisco Business Critical Services SKU CON-AS-RS-OPT which assists the Customer with issues reported for any of the technologies listed below.

Technologies Supported

- Routing and Switching
- Wireless Networking
- Network Management and Orchestration
- Computing Systems
- Storage Area Networking
- Data Center Switching
- Application Centric Infrastructure
- Data Center Orchestration and Automation
- Unified Communications
- Video Collaboration
- Network Security
- Security Policy and Access

Solutions Supported

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

Cisco Responsibilities

- Designate a Cisco Classified Network Support person (CNS Operations Manager) to act as the primary non-technical liaison point-of-contact to provide Deliverables and activities.
- Provide the following:
  - Case Request Escalation Management: Operations Manager will facilitate problem resolution on a reactive basis for technical issues reported to Cisco by Customer, and help Customer determine if appropriate resources are being applied to technical issues reported. This includes notifying Cisco TAC and the Cisco Engineer familiar with Customer’s Network of any planned event by pre-opening case and alerting Cisco TAC of relevant information related to the scheduled event.
  - Base Reporting Package: Operations Manager will provide standard weekly, monthly, and quarterly reporting to Customer.
  - Quarterly Operations Data Analysis: Operations Manager will conduct quarterly discussion with Customer on Deliverables and activities to review alignment with Customer business objectives. This can include reactive support contract usage, case statistics, quality issues, overall case analysis (such as Product type or case priority), Network analysis, and Return Materials Authorization (RMA) trending.
  - Extended Operational Analysis of Critical Issues: Cisco will perform operational data analysis, on critical issues by identifying Customer knowledge gaps and operational abnormalities / gaps. Cisco will provide recommendation and identify possible Solutions that Customer may elect to implement to help close knowledge and system quality gaps.
- Provide direct access to the Classified Network Support team via a Cisco-provided phone number for the following:
  - Provide case-tracking and troubleshooting where available, on an up-to twenty-four (24) hours-per-day, seven (7)-days-per-week basis as follows.
    - Severity 1 or Severity 2 calls: Response objective is within fifteen (15) minutes;
Main: Foundation Theme | Section Navigation: Operational Proficiency

- Severity 3 and Severity 4 calls: Response objective is within sixty (60) minutes during Standard Business Hours as extended therein to 8:00 am – 5:00 pm US Eastern Standard Time.

- Provide a Customer Portal for Incident Tickets
  - Classify each incident ticket based on a modified version of the US-CERT incident categories: http://www.us-cert.gov/governmentusers/reporting-requirements.
  - Prioritize all Incidents, based on information known to Cisco at the time of incident creation, into High, Medium, and Low priority based on one or more criteria such as the type of infection, confirmation of the incident, or the number assets associated with the Incident. Priorities are defined as:
    - High: Critical business impact or data loss to the Customer
    - Medium: Adverse effect to Customer, potential data loss, potential loss of service.
  - Electronically notify designated Customer contacts for new incidents.
  - Communicate mitigation recommendations if available for associated incident.
  - Note any corrective actions requiring action by the Customer including gaps in the information provided.

Additional Responsibilities
*Specifically applies only if Customer has purchased this Deliverable in conjunction with Cisco Remote Managed Services*

- Designate a CNS Operations Manager to act as the focal point for change management procedures.
- Define the high level scope of work required to transition Customer’s existing Network to readiness for management of the Managed Components by Cisco, including assessing changes required to Customer’s platform, Network and processes in order to commence the Services.
- Provide and help manage a transition plan (“Transition Plan”) that defines the overall Service transition scope, establishes milestones against which project progress will be measured, defines the requirements for establishing connectivity and access for the Service, and establishes a go-live date (or set of dates) when Cisco will begin to managed and/or monitor the Managed Components.
- Define the required inventory information and topology requirements necessary to activate or onboard the Managed Components.

Deliverables

- Case Request Escalation Management
- Base Reporting Package
- Quarterly Operations Data Analysis
- Operational Analysis of Critical Issues
- Case Tracking and Troubleshooting
- Transition Plan (this Deliverable only applies if Customer has purchased Cisco Remote Managed Services)

Optional Deliverable Bundle

With the above Deliverables, the following Optional Deliverable bundle may be added. Deliverables and activities described below are available individually, in a grouping of two optional Deliverables or in its entirety. Customer may not select greater than two optional Deliverables unless all of the optional Deliverable bundles have been selected.
Engineering Field Analysis (EFA) Coordination and Reporting: Coordinate the return of parts requiring a failure analysis and communication on the status to the Customer. Regular reporting, status, and escalation assistance will be provided.

Service Delivery Level Reporting: Provide reporting focusing on delivered Service levels.

Custom Reports: Provide custom reports in support of either service level agreement (SLA) reporting requirements or as specified by the Customer.

Onsite CNS Operations Manager: Provide a dedicated individual to perform Operations Management-related tasks at the Customer identified site for duration as specified in the Quote for Services.

**Optional Deliverable Bundle**
- EFA Coordination and Reporting
- Service Delivery Level Reporting
- Custom Reports
- Onsite CNS Operations Manager

**Limitations**
- For Case Request Escalation Management, pre-opening cases for planned event is not to exceed two (2) events per month.

**Customer Responsibilities**
- Coordinate any delivered on-site visits by Cisco, and provide minimum thirty-days (30-days) notice to Cisco of the scheduled visit; in the event the date for the scheduled visit is changed, Customer may be subject to additional charges.
- Report Severity 1 and 2 problems directly using the Cisco-provided phone number; response times do not include problems reported using Cisco.com or other electronic means.

### 3.5.1b - CNS High-Touch Technical Support (U.S. Only)

CNS High-Touch Technical Support (CNS HTTS) is a 24x7 Service that provides access to a team of network specialists who can assess and expedite issue resolution, define a solution that seeks to limit network disruption, and assist network operating staff in implementing the appropriate solution for increased availability of Customer’s mission-critical business infrastructure.

CNS HTTS will deliver all Services by United States (US) citizens, in secure US locations, with strict data access controls in place. All Customer data is stored on network with strict access controls.

**Target Customer Segment**
- US Government Agencies, or Small to Medium companies operating on classified networks.
- Non-Federal US Government Entities, or Small to Medium Companies with strict security requirements.

**Dependencies**
- In order to purchase CNS High-Touch Technical Support, CNS High-Touch Operations Management is required across Customer’s entire network.
- Depending upon the clearance level required, Service may begin thirty (30) days after acceptance of the Purchase Order.
Customers on either unclassified or classified networks, the CNS HTTS Service will be remotely delivered from the CNS secure data center, located in Research Triangle Park, North Carolina.

**Technologies Supported**

- Routing and Switching
- Wireless Networking
- Network Management and Orchestration
- Computing Systems
- Storage Area Networking
- Data Center Switching
- Application Centric Infrastructure
- Data Center Orchestration and Automation
- Unified Communications
- Video Collaboration
- Network Security
- Security Policy and Access

**Solutions Supported**

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

**Additional Information to be Collected**

- Organizational structure, solutions goals, business, technical and operational requirements.
- Security policy, security incident management process and incident handling procedures.
- Asset classification and prioritization documents.
- Information and or policies regarding normal and permissible network traffic.
- Documentation for identification, classification and prioritization of critical systems and data.
- Quarterly vulnerability scan reports which include details on listening ports, version of services, point-in-time baselines of vulnerabilities associated with critical assets such as services and software applications.
- Situations or places in the network where full packet capture may not be permissible.
- Inventory information and topology requirements, host names, IP addresses, SNMP strings, passwords, and other information necessary to activate or onboard the managed components.

**Cisco Responsibilities**

**Project Management:**

- In addition to the Cisco PM responsibilities described in the [Cisco Business Critical Services - General Terms](#), Project Manager will:
  - Define communications flow with Customer’s project sponsor and key stakeholders.
  - Review status of dependencies, risks, and issues associated with successful delivery of the Service.
  - Act as focal point for change management procedures.

**Kickoff Session:**

- Conduct a kickoff session which within forty (45) days from receipt of Purchase Order to review the activation process and activities with the Customer and create a project plan for activation of the Service.

**Transition monitoring and incident management of managed components:**

Note: Information gathering and kickoff session must be completed before commencing the transition responsibilities.
- Transition case tracking and troubleshooting responsibilities for the supported technologies as specified on the Quote.
- Execute transition plan to transition Customer’s existing network for management of the managed components by Cisco which includes the following:
  - Define a high-level scope and milestones.
  - Define the readiness requirements to establish connectivity and access to the managed components by Cisco.
  - Define the required inventory information and topology requirements necessary to activate or onboard the managed components.
  - Establish go-live date which when Cisco will begin to manage and monitor the managed components and Customer will access the Service.
- Conduct a transition out-brief upon completion of the above transition activities which will cover the following:
  - Review of incident escalation process.
  - If applicable recommendations which must be addressed based on information analyzed.
  - Service go-live date for monitoring and incident management by CNS HTTS.

**Monitoring and incident management of managed components:**
- CNS HTTS is provided remotely (not onsite) and includes providing the Customer direct access to the Federal Special Secure Support Team via a Cisco provided phone number. CNS HTTS will provide response to Customer as follows:
  - Severity 1 or Severity 2 calls: Response objective within fifteen (15) minutes.
  - Severity 3 or Severity 4 calls: Response objective within sixty (60) minutes.

**Note:** Response times do not include problems reported using Cisco.com or other electronic means.
- Provide case tracking and troubleshooting Services, where available, on a twenty-four (24) hours per day, seven (7) days per week.
- Provide 24/7 access to expert engineers, familiar with Customer’s network for faster issue resolution.
- Provide network service level support which assesses services requests beyond device level to determine and address symptoms at a network level.
- Provide a dedicated toll-free number. Customer will only be asked for Service Contract number and basic information on Customer CCO profile.
- Monitor the managed components identified in transition plan.
- Provide incident handling as follows:
  - Create incident tickets on the Customer Portal.
  - Classify each ticket based on a modified version of the US-CERT incident categories located here: https://www.us-cert.gov/government-users/reporting-requirements
  - Prioritize all incidents, based on information known to Cisco at the time of the incident creation into High, Medium, and Low priority and several criteria such as type of infection, confirmation of the incident, or the number of assets associated with the incident. Priorities are defined as:
    - High - Critical business impact or data loss to the Customer.
    - Medium - Adverse effect to the Customer, potential data loss, potential loss of service.
  - Electronically notify designated Customer contacts for new incidents.
  - Provide mitigation recommendations as available for associated incident.
  - If Cisco becomes aware of an incident, Cisco will attempt to notify the Customer designated point of contact for the Service.
Deliverable

- Transition Plan
- Transition Out-brief

Customer Responsibilities

- Collaborate with Cisco NCE to create the following if they do not exist for purposes of assisting with issue resolution and implementation of appropriate solutions:
  - Topology map with IP networks
  - Design and configuration templates
- Perform tasks identified in the Transition plan in support of activation of the Service.
- Provide reasonable electronic access to Customer’s network for Cisco to provide the Service.
- Report Severity 1 and Severity 2 problems for managed components using the Cisco provided phone number.
- Review incident tickets on the Customer Portal and provide timely information required for ticket resolution and closure.
- Implement Cisco’s recommended mitigation solutions in a timely manner in order to expedite resolution of incidents and increase availability of Customer’s mission-critical business infrastructure.

Definition of Terms Used

- **Customer Portal** – Web application provided by Cisco to Customer that details visibility into the CNS HTTS Service, including incident tickets and reports.
- **Incident Tickets** – An enumerated report that provides details about an incident detected by the CNS HTTS team and requires attention from the Customer.
- **ISO** – International Standards Organization
- **Security Incident or Incident** – A single series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security (ISO 27035).
4—THREAT MITIGATION

Threat Mitigation assists with aspects of incident readiness and response.

SECTION NAVIGATION

Foundation Theme – Threat Mitigation includes the following Service capabilities and Deliverables, each bookmarked for easier navigation:

- 4.1 – Security Incident Response
  - 4.1.1 – Incident Response Retainer

4.1 – Security Incident Response

Security Incident Response focuses on incident readiness and response to incidents through targeted activities that evaluate awareness and response process.

4.1.1 – INCIDENT RESPONSE RETAINER

Cisco Incident Response (IR) Retainer provides review and evaluation of Customer’s incident readiness program.

Architecture Supported

- Security

Additional Information to be Collected

- Incident response strategy information, including processes and workflows.

Cisco Responsibilities

- Provide any or all of the following Incident Response Deliverables as part of the retainer: incident readiness activities, incident response strategy and planning, tabletop exercises, proactive threat hunting, and emergency incident response which can include triage, coordination, investigation (such as analysis and forensics), containment, and remediation.
- Provide emergency access to Incident Response Services for the duration of the subscription.
- Use commercially reasonable efforts to (a) assign a resource within four (4) hours remotely via telephone, and (b) begin deployment of personnel to Customer location within twenty-four (24) hours.
- Provide monthly status update specific to the Customer’s environment.
Deliverables

The Deliverables for the Service may include any or all of the following:

- Incident Readiness Activities
- Incident Response Strategy and Planning
- Tabletop Exercises
- Proactive Threat Hunting
- Emergency Incident Response

Limitations

- Given the variety of situations and issues that may be encountered, incidents may require a variety of Services to complement this Service. For example, incidents may require specialized tools to provide deeper visibility or access into the Network. Other limitations include:
  - There is no guarantee that root cause analysis will result in a root cause being identified or confirmed for an incident.
  - Reasonable efforts will be made to provide conclusive findings and an issue resolution plan.
  - Incident Response Services can provide insight into deficiencies of an Incident Response strategy and a plan for resolving an incident; however, executing the plan may require follow-on Services.
  - Proactive Service needs to be requested and scheduled at least ninety (90) days before the end date of the subscription contract.
  - Work may occur after Standard Business Hours, as determined by Cisco.
  - Cisco will use commercially reasonable efforts to have personnel start travel to Customer’s location within 24 hours after receiving the written request, if visas and/or other travel requirements are not needed. If visa and/or special travel requirements are needed, Cisco personnel will continue to work remotely while travel arrangements are being made (e.g. applying for visa).
  - Cisco reserves the right to refuse travel to any location that is in Cisco’s reasonable opinion is unsafe, unlawful, or may require a forced intellectual property transfer by Cisco.
5—RELIABILITY ENGINEERING

Reliability Engineering provides Customers with a trusted advisor and On-Site consulting expertise to enhance Cisco application and infrastructure for security, reliability, manageability, performance, and operational gains.

SECTION NAVIGATION

**Foundation Theme – Reliability Engineering** includes the following Service capabilities and Deliverables, each bookmarked for easier navigation:

- 5.1 – Foundation Trusted Advisor
  - 5.1.1 – Foundation Onsite Consulting
  - 5.1.2 – Foundation Onsite Support

5.1 – Foundation Trusted Advisor

Foundation Trusted Advisor provides leadership help to enable Customers to obtain the benefits of Cisco’s Foundation capabilities with a focus on planning, coordinating, and delivering required capabilities through On Site and Remote delivery approaches.

5.1.1 – FOUNDATION ONSITE CONSULTING

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

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

**Technologies Supported**

- Routing and Switching
- Wireless Networking
- Network Management and Orchestration
- Computing Systems
- Storage Area Networking
- Data Center Switching
- Application Centric Infrastructure
- Data Center Orchestration and Automation
- Tetration
- Unified Communications
- Customer Care
- Cloud Meetings and Messaging
- Network Security
- Security Policy and Access
- Cloud Security
- Advanced Threat
- Packet Core
- Mobility Policy and Access
- SP Video Infrastructure
- IoT Edge and Fog Compute
Main: Foundation Theme | Section Navigation: Reliability Engineering

- Video Collaboration
- Hosted Collaboration Solution
- Industrial Networking and Collaboration

### Solutions Supported

- Network Service Orchestration
  - Network Management and Orchestration
  - Data Center Orchestration and Automation
- Self-Optimizing Network (SON)
  - Mobility Policy and Access
- Software Defined WAN
  - Routing and Switching
  - Network Management and Orchestration
- Virtual Packet Core
  - Packet Core

### Cisco Responsibilities

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

**Note:**

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

### Deliverables

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

<table>
<thead>
<tr>
<th>Health Insights</th>
<th>Technology Assessments</th>
<th>Security Compliance</th>
<th>Software Compliance and Remediation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Platform Insights</td>
<td>Security Compliance Assessment</td>
<td>Configuration and Software Change Support</td>
</tr>
<tr>
<td></td>
<td>Performance Tuning Support</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Capacity Assessment</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Resiliency Assessment</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Collaboration Security Assessment</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RF Verification Assessment</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>WLAN RF Assessment</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Operations Management
- Escalation Engineering Support
- Operations Risk Management Assessment
- IT Operations Model Analysis
- Operations Process or Runbook Update

Knowledge Management
- Knowledge Transfer Session

Instrumentation Management
- Management Instrumentation Review
- Management Deployment Planning and Readiness Assessment

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

5.1.2 – FOUNDATION ONSITE SUPPORT

Foundation Onsite Support is provided at Customer’s designated location up to five (5) days per week (pending local work restrictions).

Foundation Onsite Support is only available in certain geographic locations and will be specified in the Quote for Services.

Solution Supported
- High-Touch Expert Care

Cisco Responsibilities
- The responsibilities provided by Foundation OnSite Support are defined within the following Foundation Deliverables described above.

<table>
<thead>
<tr>
<th>Operations Management</th>
<th>Incident Management</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Problem Management- High-Touch Engineering</td>
</tr>
</tbody>
</table>

Note: Cisco may deem it necessary to provide specific Deliverables through a combination of On Site Support and Remote-support.

Deliverables
- Onsite Support Incident Management
- Onsite Support Problem Management High Touch Engineering

Note: The Quote will specify the Foundation Onsite Support Deliverable(s) purchased.

Customer Responsibilities
Provide Cisco with direction of support activities and priorities on which the Customer needs Cisco Support to engage.