# SERVICE CATALOG

## Network Operations Center (NOC)

## Desktop Optimization Center (DOC)

## Security Operations Center (SOC)

# Table of Contents

Why NOCDOC Network Operations Center (NOC) and Service Desk Services ..... 6
Account Management ..... 7
Grow your business without extending your payroll ..... 7
Sizing and Pricing ..... 8
F: Fault Management ..... 8
C: Configuration Management ..... 8
A: Accounting Management ..... 9
P: Performance Management ..... 9
S: Security Management ..... 9
Transition Management ..... 10
Simple Onboarding ..... 10
Standardized Onboarding Procedures ..... 10
Timeline and Schedule ..... 10
Assess – 2 days ..... 10
Plan – 3 days ..... 11
Design – 2 Days ..... 11
Installation/Implementation 12.5 Days ..... 12
Documentation/Knowledge Management - 7.5 Days Concurrent ..... 12
Go/No Go Decision – Day 28 ..... 12
Go-Live ..... 12
Service Operations ..... 13
Early Life Support ..... 13
Continual Service Improvement ..... 14
Improvement Initiatives ..... 14
Improvement Stages ..... 14
Network Operations Center (NOC) Overview: ..... 15
Monitoring Methods ..... 15
Operational Processes ..... 16
ITIL Operational Processes – Roles & Responsibilities ..... 16
ITIL Operational Processes - Detailed Controls & Mechanisms ..... 17
'Level 1: Respond ..... 18
Monitoring & Event Management ..... 18
Event Management ..... 19
Level 2: Remediate ..... 22
Standardized Processes ..... 22
Incident Management ..... 22

Problem Management ..... 23
Configuration Management ..... 24
Change Management ..... 25
Release Management ..... 25
Level 2 Engineer Roles & Responsibilities ..... 27
Service Level Management ..... 27
Level 3: Resolve ..... 28
Capacity & Performance Management ..... 28
Standardized Processes ..... 28
Capacity Management: ..... 28
Performance Management: ..... 28
Level 3 Subject Matter Expert Roles & Responsibilities ..... 29
Service Level Management ..... 29
Level 2+: Service Level Management ..... 30
Reporting: ..... 30
NOC Services Features Overview: ..... 31
Service Desk (SDX) Overview: ..... 32
Access via Email / Chat / Web / Phone ..... 32
Branding & Integration ..... 32
Knowledgebase Management ..... 32
Service, Details & Execution (SDX): ..... 33
Service ..... 33
Details ..... 34
Execution ..... 35
*Green Team* ..... 35
Service Level Agreement ..... 36
NOCDOC Security Operations Center ..... 37
Introduction ..... 37
01 – Inventory and Control of Enterprise Assets ..... 38
02 – Inventory and Control of Software Assets ..... 39
03 – Data Protection ..... 39
04 - Secure Configuration of Enterprise Assets and Software ..... 39
05 – Account Management ..... 40
06 – Access Control Management ..... 40
07 – Continuous Vulnerability Management ..... 41
08 – Audit Log Management - SOC ..... 41

09 – Email and Web Brower Protection ..... 42
10 – Malware Defense..... 42
11 – Data Recovery ..... 43
12- Network Infrastructure Management ..... 43
13- Network Monitoring and Defense..... 44
14 – Security Awareness and Skills Training ..... 44
15 – Service Provider Management ..... 44
16 – Application Software Security ..... 45
17 – Incident Response Management..... 45
18 – Penetration Testing ..... 45

# Table of Figures

Figure 1: NOCDOC Price List for NOC & Service Desk ..... 7
Figure 2: FCAPS Model ..... 8
Figure 3: Transition Management & Early Life Support ..... 10
Figure 4: Service Center and Onsite Manager Connectivity ..... 11
Figure 5: Challenges during Early Life Support ..... 13
Figure 6: Solutions for Early Life Support ..... 13
Figure 7: CSI Feedback Cycle ..... 14
Figure 8: NOC Operations Overview ..... 15
Figure 9: Operational Processes - Roles & Responsibilities ..... 16
Figure 10: Operational Processes - Mechanisms & Controls ..... 17
Figure 11: Monitoring Methods ..... 18
Figure 12: Typical Level 1 Alert Types ..... 20
Figure 13: Problem Management Workflow ..... 23
Figure 14: Change Management Workflow ..... 26
Figure 15: Service Desk Methods of Contact ..... 32

# Why NOCDOC

## Network Operations Center (NOC), Security Operations Center (SOC) and Service Desk Services (SDX)

NOCDOC's NOC, SOC and Service Desk services are designed to accelerate MSPs' businesses by offering 24x7x365 NOC, SOC, and Service Desk services. MSP's can extend their capacity with always on and highly scalable services, without increasing their internal resources. When coupled with NOCDOC Remote Monitoring and Management (RMM), our NOC and Service Desk can seamlessly monitor, manage, and support your customers based on the policies applied in NOCDOC RMM.

NOCDOC's SOC services are aligned with NIST and CIS Controls. We take a layered approach to securing your business in accordance with the 18 controls and recommend and implement the latest technologies that are aligned with the client needs.

NOCDOC's NOC and Service Desk services is straight-forward when sizing and pricing services. During the onboarding process, NOCDOC will engage the NOC and/or Service Desk service(s) to all managed devices, groups, import and apply policy modules, scripts, and reports for subscribed sites. In addition, your Professional Services Automation (PSA) system can be integrated to ensure that your team will receive notifications when new tickets are created, updated, solved or escalated.

NOCDOC offers two levels of NOC services for workstations, and three levels of NOC services for core infrastructure devices such as physical server, virtual servers, and network devices of any size or complexity. MSPs can work with their customers to determine which device type will be subscribed to the NOC services and the level of service required.

For end-user support, MSPs can deliver a Service Desk offering to their clients with a team of trained analysts, engineers and subject matter experts that are 100% US based. The Service Desk offering can designed to fit your clients hours of coverage by a choice of standard hours (M-F 6a-8p EST), extended hours (M-F 6a-12a), or full 24x7 Service Desk support.

# Account Management

Optimize and grow your service offerings with a security-centric RMM that allows you to assess, proactively address, and deliver multilayered security services all from a single platform.

A requirement for NOCDOC's NOC and Service Desk offering is to allow NOCDOC to purchase, implement and use Barracuda's Remote Monitoring and Management toolset. If using a competitive RMM tool, the MSP can begin with an introductory offer to test the functionality of the software, processes and service delivery.

## Grow your business without extending your payroll

Your Account Manager can help you design a program that will properly support your clients without the need to develop a staffing plan. Chose the devices that should be monitored, managed, analyzed or optimized. Choose Level of Service and We will develop a budget aligned to your business needs.

| Premium<br>Core NOC Services per unit | Level 1 – Respond<br>Monitoring & Event Management | Level 2 – Remediate<br>Incident & Problem Management | Level 3 – Resolve<br>Capacity & Performance Management |
|---|---|---|---|
| Workstations | | Select Quantity | Price Per Device |
| Server/Virtual Server | | Select Quantity | Price Per Device |
| Network Device L1/L2 – Core Infrastructure<br>L1 - Access Switches<br>L2 – Firewalls, Small/Branch Office (<25 Users) | | Select Quantity | Price Per Device |
| Network Device L3 – Core Infrastructure<br>L3 – Next Generation Firewalls,<br>L3 – Storage Area Networks<br>L3 – Consolidated Backup Systems (Veeam, Datto) | | Select Quantity | Price Per Device |
| **Service Desk** | **Service Description** | **Price Per User** | |
| Premium Service Desk<br>Standard Hours | Monday-Friday<br>(6am - 8pm EST)<br>unlimited incidents | Number Users | Will price per user |
| Premium Service Desk –<br>Extended Hours | Monday-Friday<br>(6am - 12am EST)<br>unlimited incidents | Number Users | Will price per user |
| Premium Service Desk -<br>Full Support | 24 / 7 / 365 support<br>unlimited incidents | Number Users | Will price per user |
| 1-year SDX Bundle | 24x7 Service Desk +<br>Level 2 Workstation | Number Users | Will price per user |
| 2-year SDX Bundle | 24x7 Service Desk +<br>Level 2 Workstation | Number Users | Will price per user |
| 3-year SDX Bundle | 24x7 Service Desk +<br>Level 2 Workstation | Number Users | Will price per user |

*Figure 1: NOCDOC Price List for NOC & Service Desk*

## Sizing and Pricing

The chart below is a framework that should help clarify definitions on the level of service required for each device type. FCAPS is a standards-based model to define proactive monitoring and management. It was created by International Standardization Organization (ISO) over 30 years ago, to help Service Providers easily understand the way monitoring and management systems work and perform. Furthermore, FCAPS assists IT professionals when evaluating tools capacities and functions.

FCAPS is an acronym for fault, configuration, accounting, performance, security, the management categories into which the ISO model defines network management tasks.

| NOC L1 | NOC L2 | NOC L2+ | NOC L3 | SOC L1/L2 |
|---|---|---|---|---|
| **F**ault Management | **C**onfiguration Management | **A**ccounting Management | **P**erformance Management | **S**ecurity Management |
| Monitoring | Failures Remediation | Track Service Usage | Utilization Analysis | Access |
| Alert Generation | Restoration | Limits | Error Frequencies | Controls |
| Alert Handling | Initialization | Costs | Performance Data | Behavior |
| Alert Filtering | Provisioning | Quotas | Data Analysis | Log Analysis |
| Fault Detection | Auto Discovery | Audits | Capacity Planning | Alarms and Events |
| Fault Isolation | Backup Restore | Reporting | Problem Reporting | Data Privacy |
| Fault Correction | Patch Management | Management Support | Root Cause Analysis | AV/Malware |
| Diagnostic Tests | Maintenance Reboots | Ad-Hoc Report Creation | Data and Statistics | CERT |
| Error Logging | Change Management | Analysis | Maintain Logs | Rights |
| Error Handling | Software Distribution | Governance | | Breaches & Attempts |
| Error Statistics | Inventory Management | | | CIS/NIST Compliance |
| Clear Correlations | Asset Management | | | Awareness |
| Network Recovery | Automation Jobs | | | Data Loss Prevention |

*Figure 2: FCAPS Model*

## F: Fault Management

Fault Management consists of detecting problems (faults) in the core infrastructure. It is not a simple process; it is a set of practices like fault detection, isolation, correlation, and resolution. The idea is to avoid long downtime and even worst-case scenarios.

Alerts generated within NOCDOC RMM will create a trouble ticket via API to the NOC, a corresponding ticket is generated within the MSP's PSA system. The NOC team will be responsible for resolution unless the resolution requires onsite coordination or specialized knowledge about the device is required. Subsequent analysis is fundamental to implement improvements and identify behaviors, trends, correlations, etc.

## C: Configuration Management

To ensure the proper functioning of a network it is of utmost importance to have its devices properly configured. This is a continuous process, as the infrastructure grows or evolves.

Core Infrastructure configuration management requires the combined team to accurately execute, track and inventory core infrastructure configuration changes, circuits and/or path provisioning, as well as ensure a seamless expansion.

## A: Accounting Management

Also known as billing management. Is a FCAPS level that brings you network usage data and parameters, as well as a comprehensive network inventory. It is the responsibility of the Managed Service provider to provide Accounting Management. Becoming familiar with the sets of reports available in NOCDOC is critical to provide clients with key information and progress in the client's environment.

## P: Performance Management

This level provides real-time and historical network performance information, as well as helping network operators ensure that the network is running as expected.

The network performance aims to guarantee efficient network functioning by means of monitoring several parameters such as a circuit performance, through input and output, percentage utilization, error seconds… This way, you are provided with statistics data that can be used to improve your fault management processes, network performance and behavior, as well as meet SLA requirements.

NOCDOC RMM will be able to monitor SNMP, WMI and Windows Performance Counters and SSH for Linux/Unix and macOS systems. Additional complimentary solutions may be required to provide performance data such as flow control, packet sniffing, network analyzation and bandwidth historical graphing within a client's infrastructure.

## S: Security Management

Security management is a complex level aiming to protect the network against cybersecurity threats and attacks. This involves practices such as network assets and consumption control, access management and unauthorized access monitoring, log activity control, end-point protection, user permissions management, etc. Most of these functions can be monitored through NOCDOC RMM and will alert on authentication incidents.

In order to offer advanced Security Management, additional tools and services will be required. NOCDOC's existing portfolio of email, network, and application security products will provide a broader set of tools to help become a security-centric MSP. Security Incident Event Monitoring (SIEM) and Security Operations (SOC) services can be added to increase threat monitoring and help clients become more secure.

# Transition Management

## Simple Onboarding

NOCDOC will guide the MSP to set up Service Center and the collection of managed devices, into proper site and service groups. There is an existing integration from NOCDOC RMM to the most common PSA systems for ticket management. The Network Operations Center (NOC) will leverage the Service Center integration as a central hub between the ticketing systems. Service Desk integrations will be a separate integration from the MSP branded Zendesk ticketing system and the MSP's existing PSA system.

## Standardized Onboarding Procedures

NOCDOC has developed a standardized methodology for Onboarding MSP's and clients for over 10 years and over 1000+ sites. Our standards-based approach is developed from Project Management Institute (PMI) and Information Technology Infrastructure Library (ITILV4) best practices for Service Transition Management. Below is a sample diagram to focus on the first 60 days of operation from Service Order through Service Transition.

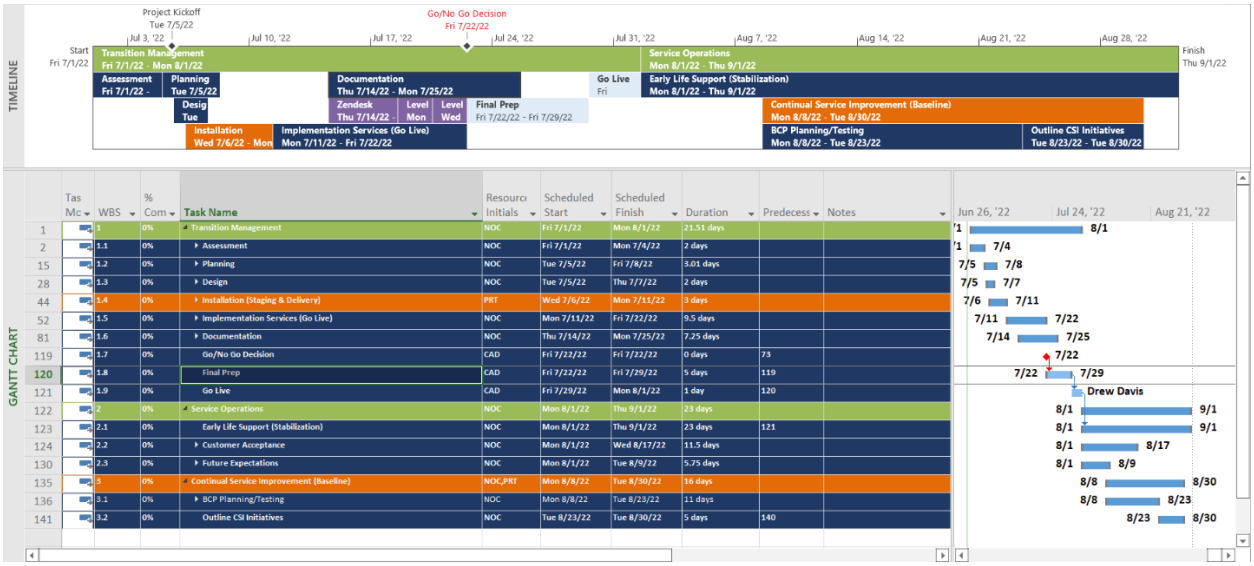



*Figure 3: Transition Management & Early Life Support*

## Timeline and Schedule

### Assess – 2 days

NOCDOC's Onboarding Manager will coordinate with the MSP Point of Contact (POC) to provide a kickoff date and develop to overall Transition Schedule. The MSP Point of Contact can be the liaison to the client or include the client in the transition process. Set proper expectations that the transition period will be a 30-day period from the time the Service Order is received until the Go-Live Date. It is our best practice to start Go-Live dates on Mondays.

- ☐ Purchase Order Processed
- ☐ Service Order Commencement
- ☐ Alignment with Service Order
- ☐ Submit Order for Zendesk Spoke
- ☐ Contact List Established – MSP and Client
- ☐ Organize Kick-off Call with MSP and Client

## Plan – 3 days

Access to tools and knowledge base information begins to form during the Planning Stage. Key stakeholders are scheduled to attend a kick-off call and the exchange of information begins during this stage.

- ☐ Access to Service Center
- ☐ Action Register Prepared
- ☐ Establish Timelines
- ☐ Set Expectations
- ☐ Provide MSP Access to IT Glue
- ☐ Provide NOC and Service Desk Questionnaires
- ☐ Kick-off Call with Client and MSP

## Design – 2 Days

During the Design Phase, decisions about monitoring methods and Site Management configurations are defined. In the case of the first client for a Managed Services Provider a new Zendesk instance will be ordered and configured. Specific details about branding and email communications are established. If the MSP has not already configured previously, integration between NOCDOC RMM and MSP's PSA system is configured.

- ☐ Monitoring Design – Onsite Manager and Device Managers
- ☐ Establish Site Management configurations
- ☐ Configure Zendesk Spoke
- ☐ Establish Ticketing System Queues
- ☐ Import Zendesk end-user list
- ☐ Configure Service Center Integration to Service Center

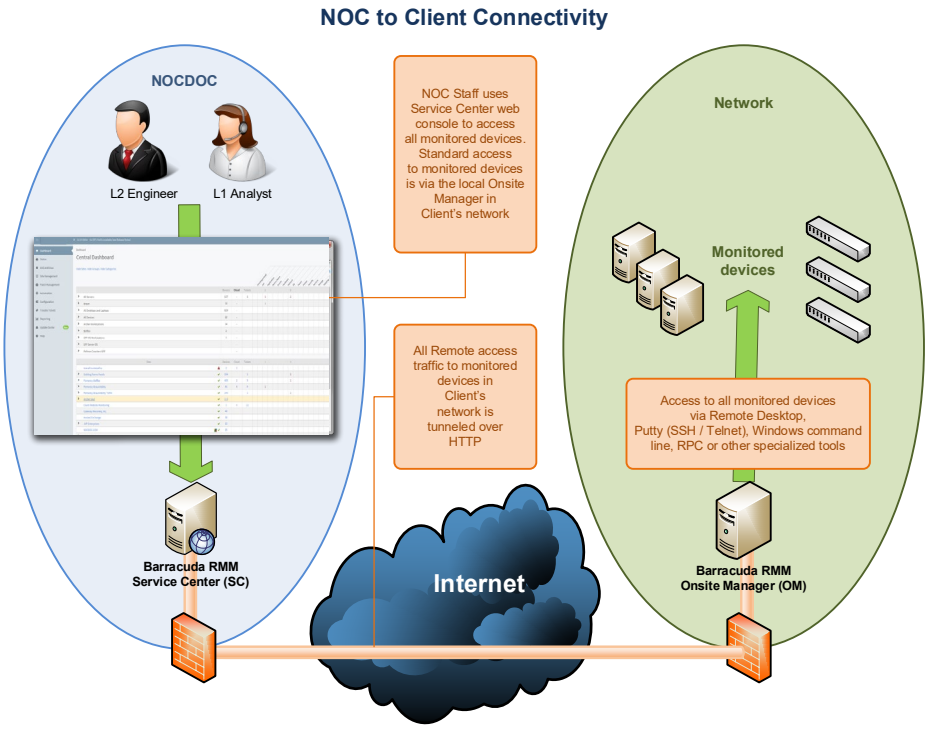



*Figure 4: Service Center and Onsite Manager Connectivity*

## Installation/Implementation 12.5 Days

The MSP determines the quantity of devices to be monitored and level of service as defined in the RMM Service Catalog. Each device will be provided a set of policy modules that represent Best Practices in equipment alert configurations for FCAPS.

Policy Modules are typically a set of monitor types such Availability, Network Services, Bandwidth, SNMP Gets, SNMP Traps, Syslog Messages and WMI. Provider will deploy a collector server for agentless or device agent for isolated devices to collect SNMP, WMI, and Log File information. Depending on the level of service the RMM team will work with the FCAPS model to monitor, restart, remediate, and restore selected devices.

- ☐ Deliver Onsite Manager to client location
- ☐ Configure Hardware and Software
- ☐ Establish connectivity to the Service Center
- ☐ Setup Network Discovery Scans
- ☐ Define and apply Policy Modules/Sets
- ☐ Develop Custom Policy Modules if necessary
- ☐ Modify aliases for Ticketing

## Documentation/Knowledge Management - 7.5 Days Concurrent

The Best Practice for capturing documentation will be to import and populate asset information into industry leading Knowledge Management tool IT Glue. For those MSP's that already utilize IT Glue we will set up the sharing request to integrate Glue Connect between the two IT Glue instances. For MSP's who have not adopted IT Glue, NOCDOC will provide Lite Agent Access into our instance of IT Glue with read-only capabilities into the list of clients managed by the MSP.

- ☐ Document Executive Summary into IT Glue
- ☐ Document Client Profile with Key Contacts, Locations
- ☐ Document Escalation Policy
- ☐ Document Core Assets
- ☐ Document Applications/Services
- ☐ Document Service Desk Knowledgebase Articles

## Go/No Go Decision – Day 28

During the fourth week of Transition Management, there we will be collaborative review of the systems and documentation in all systems. An evaluation of documentation completeness and a gap analysis of what information may need to be gathered or finalized prior to Go-Live will be published. Agreement between the MSP, NOCDOC and Client is critical prior to a Go Live Decision. If the Gap Analysis in the Action Register demonstrates that the risk is too high, then the Go-Live will likely be pushed 1 week.

## Go-Live

Go-Live is considered a milestone when service is available to the general population. Most typically we recommend that Go-Live dates are scheduled for a Monday for convenience to the end-user community. Communication plans can be developed to inform end-users when the new service will begin and most-often an incumbent service will be ending. Go-Live dates also represent the date when the site will begin the billing process. Go-Live also signifies the end of Transition Management and the beginning of Service Operations.

# Service Operations

## Early Life Support

The first 30-60 days of a Managed Services engagement are the most critical to the success of a long-term engagement. There may be transition of roles and responsibilities internal to the Managed Services Provider and/or the Client that can create additional complications to engagement.

It is important to have a thorough understanding of the possible Challenges associated with Transition and the Solutions we recommend stabilizing the account and develop positive relationships starting at Go-Live.

*Challenges*

| FORMING | STORMING | NORMING | PERFORMING |
|---|---|---|---|
| BEHAVIORS | BEHAVIORS | BEHAVIORS | BEHAVIORS |
| The purpose and goals for the team are unclear | Differences and confusion arise over goals and roles. | Team gains confidence, feels a sense of momentum. | Members take full responsibility for tasks and relationships. |
| Members feel varying degrees of commitment. | Struggles erupt over approaches, direction, and control. | "What", How", "Who", and "When" become clarified. | Team achieves effective and satisfying results. |
| Members are cautious, don't initiate and avoid responsibility. | Team members react toward leadership with counterproductive behaviors. | Team develops agreements on approaches, goals, communication, and leadership roles. | Team takes the initiative to continually assess external forces. |
| Communication is low and a few members often dominate. | Team is uncertain about how to deal with issues openly. | Team builds relationships with externals (customers, key stakeholders) | Team facilitates itself easily through the various stages. |
| Members are dependent on directive leadership. | Team wrestles with issues of communication. | Members begin to relate interdependently. | Members work proactively for the benefit of the team. |
| | Members act from an independent stance. | | |

*Figure 5: Challenges during Early Life Support*

*Solutions*

| FORMING | STORMING | NORMING | PERFORMING |
|---|---|---|---|
| TASKS | TASKS | TASKS | TASKS |
| Build a common purpose. Clearly establish the expectations of the customers or sponsors. | Involve everyone in the discussion. | Develop processes for information sharing, feedback, and resource distribution. | Continuously seek to improve tasks and relationships. |
| Understand personal expectations and interests. | Inquire into differences; include all ideas and opinions. | Have open forums on tasks and relationships, both internal and external. | Assess and evaluate results against purpose and external forces. |
| Clarify accountability, recognition, and rewards. | Seek further clarity about purpose and develop a common approach to meeting project objectives. | Build appropriate feedback loops with external relationships. | Celebrate successes – reward and recognize both team and individual wins. |
| Assess resources; see who has what to contribute. | Assess and test resource needs; make necessary adjustments. | Work toward consensus on overarching issues. Negotiate where appropriate. | Continuously test for better methods and approaches. |
| Leader provides direction and drives the team process | Define operational agreements. | Leader uses a facilitative style to create the opportunity for others to lead. | Leader focuses on purpose, interdependent relationships, and conditions that shift the stage. |
| | Leader raises difficult issues and coaches team through struggles. | | |

*Figure 6: Solutions for Early Life Support*

## Continual Service Improvement

Continual service improvement, defined in the ITIL continual service improvement model, CSI aims to align and realign IT services to changing business needs by identifying and implementing improvements to the IT services that support the business processes. It incorporates many of the same concepts articulated in the Deming Cycle of Plan-Do-Check-Act. The perspective of CSI on improvement is the business perspective of service quality, even though CSI aims to improve process effectiveness, efficiency and cost effectiveness of the IT processes through the whole lifecycle. To manage improvement, CSI should clearly define what should be controlled and measured.

There needs to be upfront planning, training and awareness, ongoing scheduling, roles created, ownership assigned, and activities identified to be successful. CSI must be planned and scheduled as process with defined activities, inputs, outputs, roles and reporting.

## Improvement Initiatives

Improvement initiatives typically follow a seven-step process:

- Identify the strategy for improvement
- Define what you will measure
- Gather the data
- Process the data
- Analyze the information and data
- Present and use the information
- Implement improvement

## Improvement Stages

- Transition – 60 Days
- Stabilization – 90 Days
- Assessment – 120 Days
- KPI/CSI – 180 Days
- Transformation – 1 Year

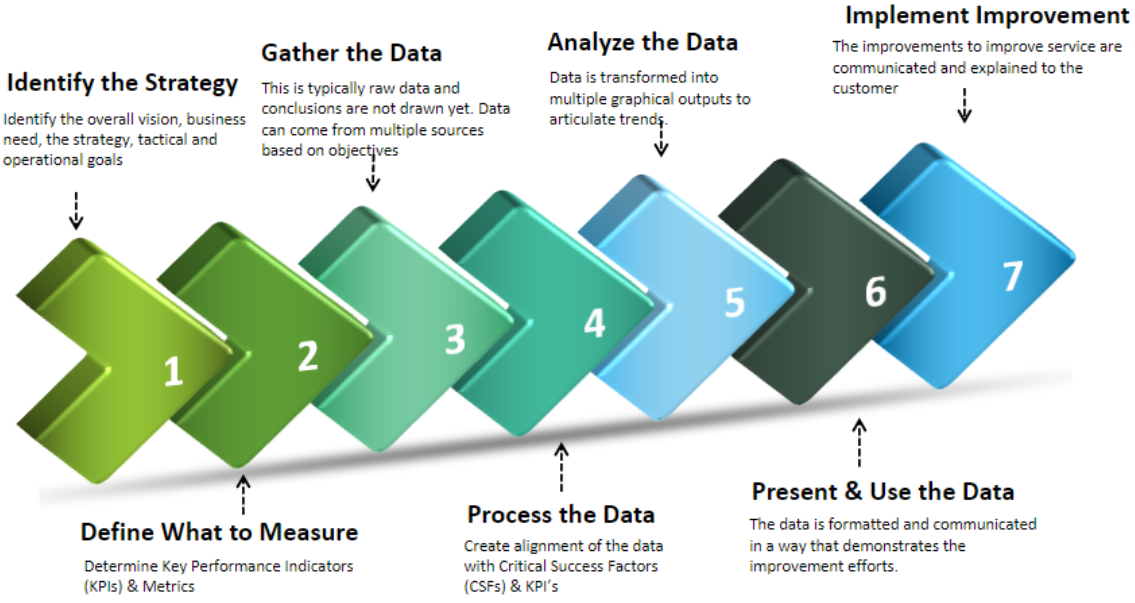



*Figure 7: CSI Feedback Cycle*

# Network Operations Center (NOC) Overview:

NOC Services at a high-level includes configuration of Monitoring Methods, generation of alerts into an IT Service Management system, Standardized Processes for Event, Incident, Problem, Change and Request Management and Business Intelligence through Dashboard Analytics.

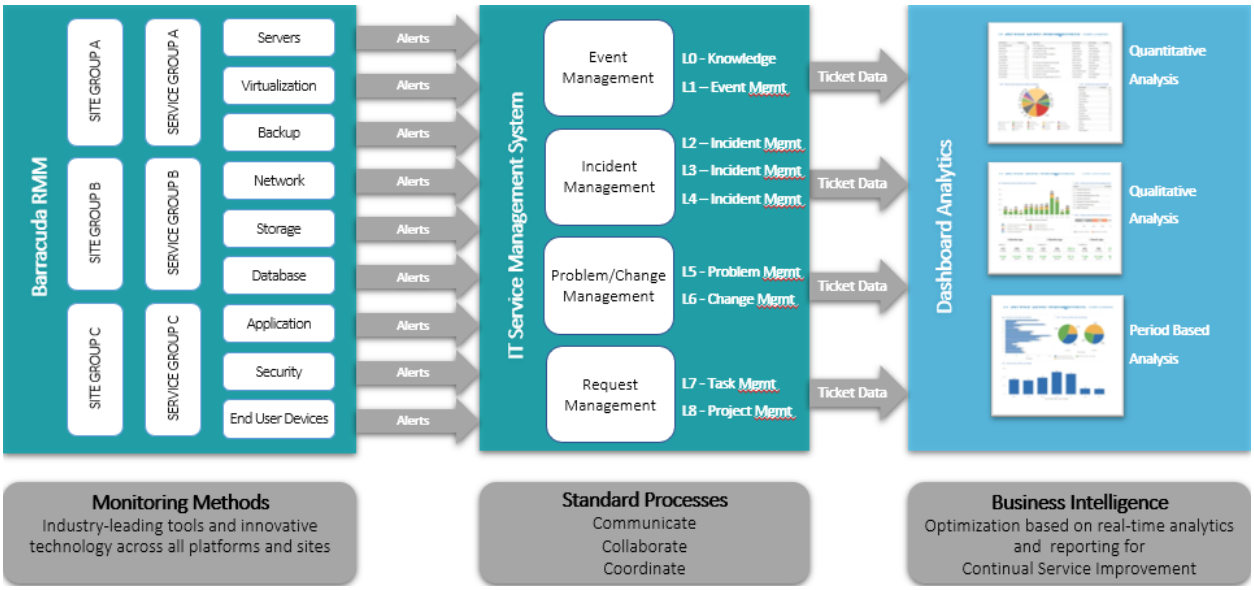



*Figure 8: NOC Operations Overview*

## Monitoring Methods

### *IT Asset Management*

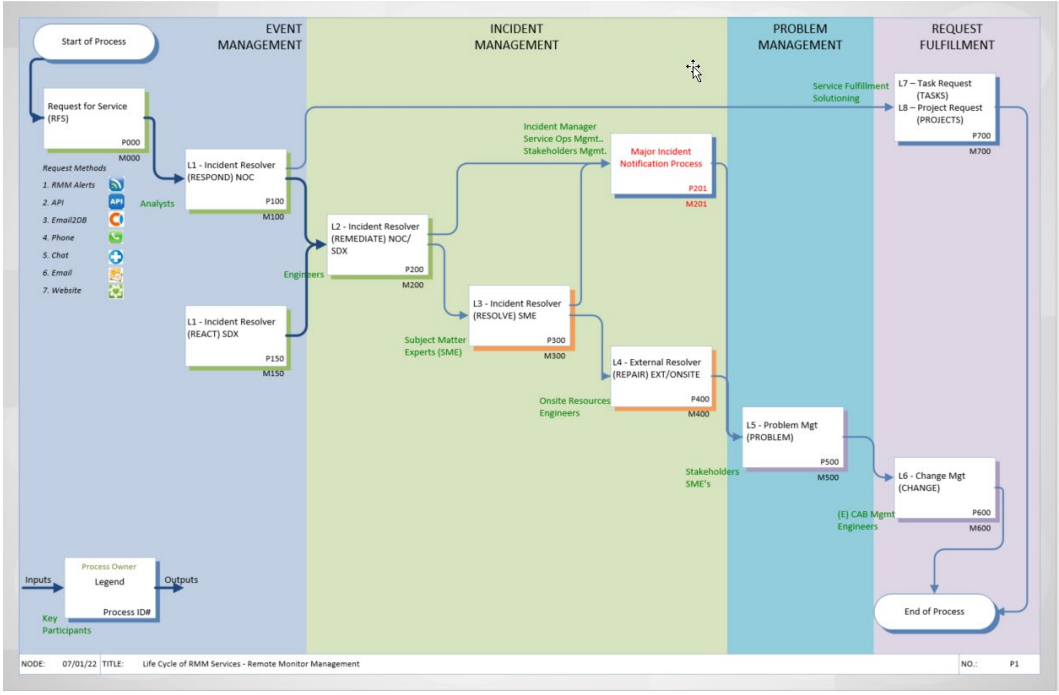
Asset inventory will be provided as part of NOCDOC RMM solution, which includes hardware and software inventory, software metering, and asset warranty reporting. The ability to connect the asset inventory data to most ITAM (IT Asset Management) systems and/or CMDB-based solutions is an option that can also be provided if needed.

The asset inventory solution enables inventory and management software license usage throughout NOCDOC's RMM by using an online software title catalog. Reports are available to the MSP through the Service Center included in the solution present this information in easy-to-use format. Many of these reports link to more specific reports that can query for general information and drill down to more detailed information. In addition, custom information can be added to the online software title catalog, such as custom software categories, software families, software labels, and hardware requirements.

- Core infrastructure and end points can be added to the Site Management within NOCDOC RMM via Network Discovery.
- Devices being monitored and alerted will have an alias designation as a prefix to the Device Name. For example:
    - MWNOC = Managed Workplace Network Operations Center which is the servicing team.
    - NA = North America where the service is being delivered.
    - L1 = Level 1 Respond is the designated level of service.
    - MWNOC-NA-L1-DEVICENAME

# Operational Processes

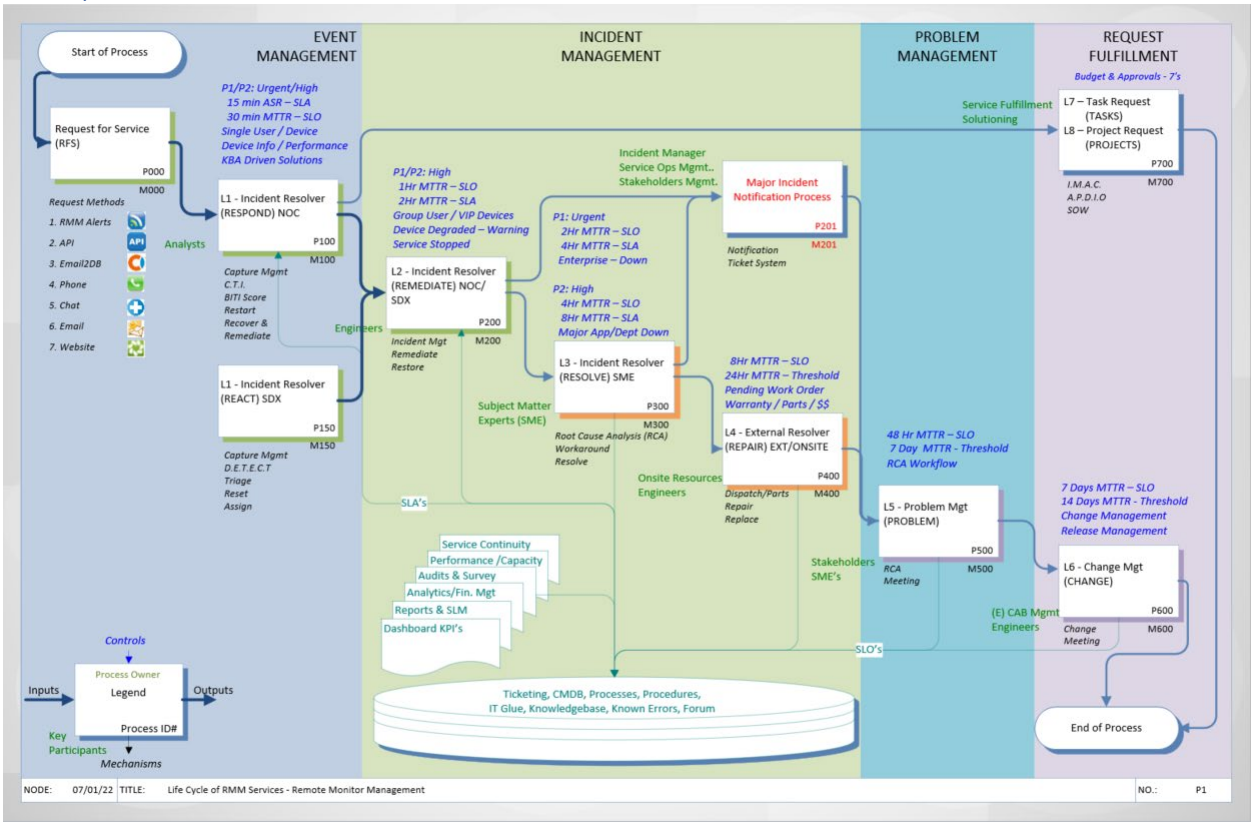
## ITIL Operational Processes – Roles & Responsibilities




| Service Management Practices in ITIL 4 include: | | Roles & Responsibilities |
|---|---|---|
| L0 | Business Analysis | Managed Services Provider |
| L0 | Service Catalogue Management | Managed Services Provider & NOCDOC NOC/SDX |
| L0 | Service Design | Managed Services Provider & NOCDOC NOC/SDX |
| L0 | Service Level Management | Managed Services Provider & NOCDOC NOC/SDX |
| L0 | IT Asset Management | Managed Services Provider & NOCDOC NOC/SDX |
| L1 | Availability Management | Managed Services Provider & NOCDOC NOC/SDX |
| L1 | Service Continuity Management | Managed Services Provider & NOCDOC NOC/SDX |
| L1 | Monitoring and Event Management | NOCDOC NOC |
| L2 | Service Desk | NOCDOC SDX |
| L2 | Incident Management | NOCDOC NOC |
| L3 | Capacity and Performance Management | Managed Services Provider & NOCDOC NOC/SDX |
| L4 | Onsite Incident Management | Managed Services Provider |
| L5 | Problem Management | Managed Services Provider & NOCDOC NOC |
| L6 | Change Management | Managed Services Provider & NOCDOC NOC |
| L7 | Service Request Management | Managed Services Provider & NOCDOC SDX |
| L8 | Project/Release Management | Managed Services Provider & NOCDOC NOC & SDX |
| L8 | Service Validation and Testing | Managed Services Provider & NOCDOC NOC & SDX |
| L8 | Service Configuration Management | Managed Services Provider & NOCDOC NOC & SDX |

*Figure 9: Operational Processes - Roles & Responsibilities*

## ITIL Operational Processes - Detailed Controls & Mechanisms




| Service Management Practices in ITIL 4 include: | | Mechanisms | Controls |
|---|---|---|---|
| L1 | Monitoring and Event Management | Capture Management<br>Event Response | |
| L1 | Service Desk | Capture Management<br>DETECT | |
| L2 | Incident Management | Incident Management Remediate | |
| L3 | Capacity and Performance Management | MSP - Performance Mgmt Tools<br>NOCDOC SME - Analysis | |
| L4 | Onsite Incident Management | MSP – Dispatch Parts/Service Order<br>NOC/SDX – Escalate REPAIR | |
| L5 | Problem Management | RCA Meeting | |
| L6 | Change Management | Change Meeting | |
| L7 | Service Request Management | MSP - Software/Hardware availability<br>NOCDOC SDX – Request Fulfillment | |
| L8 | Project/Release Management | MSP -Project Plan<br>NOCDOC NOC/SDX Implementation | |
| L8 | Service Validation and Testing | MSP -Testing Plan<br>NOCDOC NOC/SDX Implementation | |
| L8 | Service Configuration Management | MSP -Testing Plan<br>NOCDOC NOC/SDX Implementation | |

*Figure 10: Operational Processes - Mechanisms & Controls*

# ‘Level 1: Respond

## Monitoring & Event Management

Provide your customers peace of mind with 24x7 monitoring for the health, availability, and performance of their IT infrastructure. Our NOC services offers diagnostic service for the workstations, servers, network, and other core infrastructure devices selected at the monitored site. We provide diagnostics for alerts generated from NOCDOC RMM, as well as resolution steps on how the issue was remediated. With the Monitoring & Event Management service, you receive:

- Monitoring & Event Management occurs through a NOCDOC RMM Service Center which is accessible by the MSP staff. The Service Center provides real time information about monitored equipment, and it provides a dashboard overview of the client environment and alerts on a per device and aggregate view.
- Tickets can be entered by calling the Network Operations Center service number 336.714.2270, or by emailing support@nocdoc.zendesk.com . Trouble tickets are automatically generated by alerts for devices that have a MWNOC alias designation to distinguish overall devices and devices under contract
- Access to the Service Center is setup in User Configuration within NOCDOC RMM. It is the responsibility of the MSP to maintain the user configuration for internal users, extended partners, and clients with role-based access and the Sites applicable for visibility.
- The MSP can designate client Points of Contact (POC) within the Escalation Policy to have access to the ticketing system to view the status of tickets created by themselves and all tickets within their organization, including any remediation notes from NOC personnel.
- As tickets are entered into the system, knowledge base articles specific to your organization will continue to be built. Authorized staff will be able to access the knowledge base to search for known issues solved in previous tickets and view the remediation steps taken for prior occurrences. This provides a central repository for issue resolution in their environment and incident tracking and reporting.
- Note: The Average Handle Time (AHT) per ticket for Level 1 Analyst to evaluate, resolve or escalate is less than 30 minutes. Therefore, the expectation for a Level 1 Analyst is to work within the NOCDOC RMM console and not log in directly to core infrastructure with elevated privileges.
    -

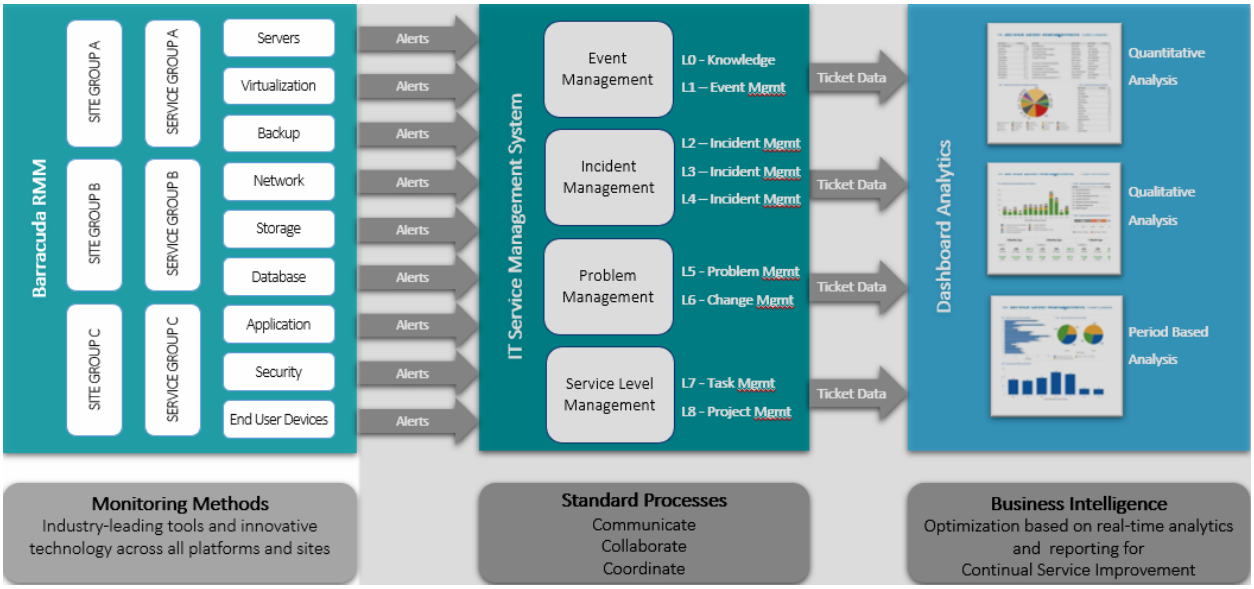



*Figure 11: Monitoring Methods*

### *Monitoring Policies*

Policy Modules are Best Practices sets of monitoring and alerting rules that NOCDOC RMM develops in partnership with leading hardware and software vendors so that out-of-the-box, the NOC can leverage best-in-class management for the IT environment. This helps accelerate the set-up time for each customer site.

Although NOCDOC RMM has an extensive library of Policy Modules, the policies are specific to Make, Model & Brand of equipment and the version levels of Operating Systems. In the case that a standard Policy Module is not applicable for a discovered device, it is necessary to develop a Custom Policy Module to properly identify the Object Identifier (OID) and then set conditions accordingly.

### *Alert Priorities*

Alert monitors are pre-set with alert priorities which help with integration and eliminating human decisions to define the priority of a ticket.

- **P1: Urgent** - An emergency condition that prevents critical business operations.
- **P2: High** - A condition that significantly impairs the use of one or more applications or systems to perform any critical business operations.
- **P3: Normal** - One or more applications or systems are affected, but the impact on business operations is not severe.
- **P4: Low** - The reported issue does not substantially impact business operations.

## Event Management

### *Level 1 Alert Types*

Diagnoses and resolution steps are tracked and managed in https://nocdoc.zendesk.com and integrated into NOCDOC RMM's Ticket Management or in integrated PSA ticketing systems

Triage and diagnose any alerts triggered in NOCDOC RMM to determine if the alert is false-positive. Typical Level 1 Respond tickets are in the following categories:

| Top 10 | Alert Type | Alert Details | Resolution Steps |
|---|---|---|---|
| 1 | Antivirus | a. Antivirus Threat Detected<br>b. Antivirus Definitions Out of Date<br>c. Antivirus Full Scan Required | a. Check Virus Chest/Quarantine status. Escalate if necessary<br>b. Trigger update request. Validate definition status<br>c. Trigger Scan and Validate results |
| 2 | Authentication | a. A user account was locked out<br>b. Account failed to login – Event 4625 | a. Verify user in active directory and unlock account<br>b. Verify user in active directory and unlock account, unknown user logins should be escalated Level 2. |
| 3 | Availability | a. Site Not Communicating<br>b. Server is offline<br>c. Network device is offline | a. Checking if the OM command prompt is connecting. Checking to see if the MWExpertSystem Service and OMNetworkService are started. If not escalate<br>b. Ping test from the Onsite Manager to validate internal communication. If not escalate<br>c. Ping test from the Onsite Manager to validate internal communication. If not escalate |
| 4 | Backup Success | a. Veeam back report success<br>b. Datto report success.<br>c. Other backup report success | a. Fill in metadata from the report and message "Backup successful, Event Captured for historical analysis<br>b. Fill in metadata from the report and message "Backup successful, Event Captured for historical analysis<br>c. Fill in metadata from the report and message "Backup successful, Event Captured for historical analysis |
| 5 | CPU Utilization | a. CPU is above 80% Utilization<br>b. CPU is above 90% Utilization. | a. Capture CPU utilization from Performance Monitors and monitor return to steady state and self-heal. |

| Top 10 | Alert Type | Alert Details | Resolution Steps |
|---|---|---|---|
| | | | b. Capture CPU utilization from Performance Monitors and escalate to Level 2 Engineer. Capture |
| 6 | Disk Error | a. Controller error was detected<br>b. Disk has a bad block | a. Checking the physical disk under the hardware section. That matches the physical drive number in the ticket.<br>b. Running a check disk scan “chkdsk” in the command prompt. If errors are found, escalate. |
| 7 | Disk Space | a. Low Disk Space | a. Capture drive disk GB information, run Clearing windows/temp and cleanmgr /verylow space. Escalate to add space. |
| 8 | Memory Utilization | a. Low Memory | a. Capture memory performance counter screenshot |
| 9 | Process Failure/ Utilization | a. | a.<br>b.<br>c. |
| 10 | Services | a. Service has terminated | a. Checking windows services if services are stopped or suspended. If services are suspended, start services. If not it’s not possible to start service, escalating it. |

*Figure 12: Typical Level 1 Alert Types*

*Level 1 Analysts Roles & Responsibilities*

| L1 | L1 Analysts / RESPOND | |
|---|---|---|
| Role  | **L1 Analysts** will categorize, prioritize, investigate, and validate the Incident and determine the course of action to recover / restart a device using Knowledge Base Articles, Standard Operating Procedures, or Work Instructions for Hardware / Software that has specific scripts and Service Levels associated with the device. The role of a L1 Analyst is to return the device to steady state of operations. | |
| Escalation Policy | If the L1 Analyst cannot resolve the Incident within the parameters specified, the L1 Analyst will escalate / notify the appropriate staff within the Service Manual Procedures. If the nature of the request for incident resolution is one that requires dispatch to Client, the Level 1 Analyst will execute the defined script. Service Level Objective (SLO) to escalate is 30 minutes. | |
| Skill | **Industry Certifications:** Comp/TIA A+, Server+, Network +, Security +, Storage+, Cloud Essentials | |
| RACI | **Categorize Incident:** Configuration Management Database (CMDB) Category, Alert Type | |
| | **Prioritize Incident:** Urgent, High, Normal, Low | |
| | **Validate Alert:** Login to Device, Verify Alert | |
| | **Investigate Alert:** identification and analysis of Infrastructure Management tools for Alert Item, Alert History | |
| | **Outcomes:** Recover based on Standard Operating Procedures, Restart, Evaluate, Escalate P1/P2 | |
| SLO / SLA | **Average Speed to Respond (ASR):** Objective < 15 Min; Threshold < 30 Min | |
| | **Mean Time to Resolve (MTTR):** Objective < 0.25 Hrs; Threshold < 0.5 Hrs | |

*Service Level Management*

| | **Average Speed to Respond (ASR) Time Based on Priority for 90% of Tickets** | | | |
|---|---|---|---|---|
| Premium | P1: Urgent | P2: High | P3: Normal | P4: Low |
| Service | 15 minutes | 15 minutes | 30 minutes | 30 minutes |

| | **Mean Time to Resolution (MTTR) Time Based on Priority for 90% of Incidents** | | | |
|---|---|---|---|---|
| Premium | P1: Urgent | P2: High | P3: Normal | P4: Low |
| Service | 1 hour | 2 hours | 8 hours | 24 hours |

- **P1: Urgent** - An emergency condition that prevents critical business operations.
- **P2: High** - A condition that significantly impairs the use of one or more applications or systems to perform any critical business operations.
- **P3: Normal** - One or more applications or systems are affected, but the impact on business operations is not severe.
- **P4: Low** - The reported issue does not substantially impact business operations.

# Level 2: Remediate

Incident Management

In addition to the services offered in **Respond**, NOC engineers will perform **Incident Management** diagnostics on alerts generated by NOCDOC RMM and remediate alerts without your involvement. In the rare scenario a device needs repair or replacement, a L4 Repair technician from the MSP would be required onsite. With the **Remediate** service, you receive:

- All benefits of Respond (Event Management)
- Remediate alerts based on agreed upon methods
- Configuration, incident, problem, and change management
- Patch Management of selected devices based on an agreed upon schedule with the stakeholders

## Standardized Processes

The responsibility of **Event Management** is to categorize, prioritize, investigate, and validate the Incident. The second step is to diagnose resolution and implement recovery, restart or remediation. Remediation is derived from either Standard Operating Procedures, Client provided Work Instructions, or Knowledge Base Articles.

All other remediations potentially introduce risk in a live production environment and are considered out of scope during business hours. These alert types must be escalated to Level 3 Subject Matter Experts or Level 5 Problem Management in the case of a recurring Incident.

## Incident Management

**Incident Management** is the process responsible for managing the lifecycle of all incidents. Incident management ensures that normal service operation is restored as quickly as possible, and the business impact is minimized. This includes faults and failures reported by event monitoring tools, and/or questions/inquiries reported by users (either via phone or via an Incident Record/Ticket).

An Incident is an unplanned interruption to an IT service or reduction in the quality of an IT service. Failure of a configuration item that has not yet affected service is also an incident – for example, failure of one disk from a mirror set.

**Incident Management** provides statistical data (when applicable) for future Continual Service Improvement (CSI). The data could include number of repeat incidents, incidents triggered by a change, and average incident duration before resolution among other information. These are often referred to as KPI's (Key Performance Indicators).

**Incident Management** provides inputs to remediation, repair / replacement, resolution, and restoration of service for Problem Management team as needed to assist in the identification of the underlying root cause of the incident.

**Incident Management** does NOT and is NOT responsible for performing the Root Cause Analysis or determining the Root Cause of a Problem.

## Problem Management

**Problem Management** has the purpose to minimize the adverse effect on the business caused by errors in the infrastructure. **Incident Management** is the primary service being delivered by the Network Operations Center (NOC) and is specifically concerned with restoring the service to the baseline performance as quickly as possible. Problem Management will focus on identifying the Root Cause of a Major Incident and then prescribing Best Practices on prevention of those events from recurrence.

A Problem is a condition often identified because of multiple incidents that exhibit common symptoms. Problems can also be identified from a single significant incident, indicative of a single error, for which the cause is unknown, but for which the impact is significant. It will become a Known Error when the root cause is identified, and a temporary workaround or permanent alternative has been defined.

A Subject Matter Expert will govern the technical resolution. Management personnel will govern the business impact and communication of Root Cause, Remediation Options, and Business Impact to the Technical and Business Stakeholders.

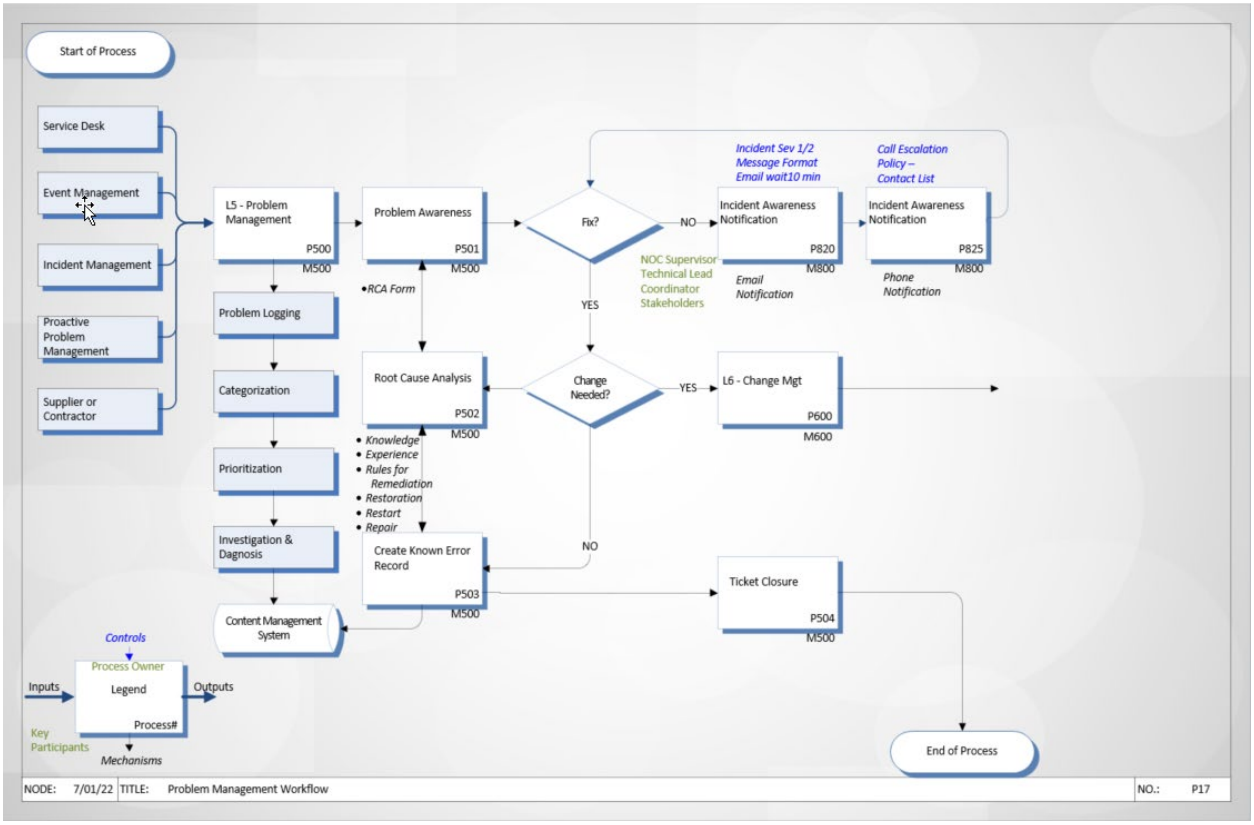



*Figure 13: Problem Management Workflow*

## Configuration Management

### *Patch Management Policy*

NOCDOC's NOC Services Patch Management Policy provides a framework for vulnerability identification, threat assessment, priority ranking, and voluntary or involuntary remediation via patch distribution by manual or automated methods.

NOCDOC's NOC Services will manage patch updates provided by all major software publishers including Microsoft and Adobe etc. For ISV software, NOCDOC's NOC Services will package all patch updates and provide test packages for the business application team to test before production rollout. Once approved, patches would be published with tasks and policies for deployment into the environment.

NOCDOC's NOC Services Patch Management Team shall identify security vulnerabilities that may impact **client's** assets and makes recommendations about the timeline for patch installation based on the threat. Patches or updates shall be applied to each host depending on the priority ranking assigned to each patch as outlined below.

### *Patch Management Best Practices*

The following guidelines apply to all Windows operating systems. Maintaining Windows OS level patches for desktop, laptop, and servers is critical to maintaining a stable and secure production environment.

- All important and critical operating system patches are to be installed according to **the client's** patch cycle
- Patch deployment would be done on rolling basis, with non-critical systems patched first to be followed by production systems
- All operating systems running past their extended lifecycle support will not be able to be patched since Microsoft no longer supports those products
- NOCDOC Services recommends upgrading from Windows 2003 server to 2012 or 2016 and from Windows 7 to Windows 10, in order to maintain compliance and security patching across **the client's** entire environment.
- All Exemptions must be approved by **NOCDOC** and fully documented

### *Priority Ranking*

All updates will be ranked, for example, as P1 through P4. Priority ranking is based on access conditions and impact of vulnerability, as well as time dependent qualities of a vulnerability such as patch and exploit availability.

- P0 – Zero day Vulnerabilities – Windows Server & Windows Clients
- P1 – One week target; Two weeks maximum – Windows Server Critical & Security Patches
- P2 – Two week target; Four weeks maximum – Windows Clients Critical & Security Updates
- P3 – Monthly or Next patch cycle – Windows Server Cumulative Patches & Rollups
- P4 – Quarterly or Discretionary – Windows Clients Cumulative & Rollups

### *Exceptions*

No scoring system is flawless and will never replace common sense. Priority adjustments need to be signed off by a management representative responsible for the asset in question and documented through a change control process for tracking purposes. At any time an alert may be created or escalated to P1 status if there is a credible risk.

## Change Management

Change Management aims to ensure that standardized methods and procedures are used for efficient handling of all changes. A change is an event that results in a new status of one or more Configuration Items (CIs), and which is approved by management, cost-effective, enhances business process changes (fixes) – all with a minimum risk to IT infrastructure.

### *Purpose of Change Management*

- Minimal disruption of services
- Reduction in back-out activities
- Economic use of resources involved in the change

### *Change Management Terminology*

- *Change:* the addition, modification or removal of Configuration Items
- *Request for Change (RFC):* aka Change Request (CR): form used to record details of a request for a change and is sent as an input to Change Management by the Change Requestor
- *Forward Schedule of Changes (FSC):* Schedule that contains details of all forthcoming changes

### *Change Management Responsibilities*

- *Hardware*
- *Communications equipment and software*
- *System software*
- *All documentation and procedures associated with the running, support and maintenance of live systems*

### *Change Management Process*

Any proposed Change must be approved in the Change Management Process. While change management makes the process happen, the decision authority is the Change Advisory Board (CAB), which is comprised of people from other functions within the organization. The main activities of the change management are:

- *Filtering changes*
- *Managing changes and the change process*
- *Chairing the CAB and the CAB/Emergency committee*
- *Reviewing and closing of Requests for Change (RFCs)*
- *Management reporting and providing management information*

## Release Management

Release and deployment management is used by the software migration team for platform-independent and automated distribution of software and hardware, including license controls across the entire IT infrastructure. Proper software and hardware control ensures the availability of licensed, tested, and version-certified software and hardware, which functions as intended when introduced into existing infrastructure. Quality control during the development and implementation of new hardware and software is also the responsibility of Release Management. This guarantees that all software meets the demands of the business processes.

### *Purpose of Release Management:*

Release management focuses on the protection of the live environment and its services through the use of formal procedures and checks.

- *Planning the rollout of software*
- *Designing and implementing procedures for the distribution and installation of changes to IT systems*
- *Effectively communicating and managing expectations of the customer during the planning and rollout of new releases*

- *Controlling the distribution and installation of changes to IT systems*

### *Release Management Terminology*

A Release consists of the new or changed software and/or hardware required to implement approved changes. Release categories include:

- *Major Software/Hardware Release: Normally contains large amounts of new functionality, some of which may make intervening fixes to problems redundant. A major upgrade or release usually supersedes all preceding minor upgrades, releases and emergency fixes.*
- *Minor Software/Hardware Release: Normally contains small enhancements and fixes, some of which may have already been issued as emergency fixes. A minor upgrade or release usually supersedes all preceding emergency fixes.*
- *Emergency Software/Hardware Release: Normally contains the corrections to a small number of known problems.*

### *Release Management Process*

Releases can be divided based on the release unit

- *Delta Release: A release of only that part of the software which has been changed. For example, security patches.*
- *Full Release: The entire software program is deployed—for example, a new version of an existing application.*
- *Packaged Release: A combination of many changes—for example, an operating system image which also contains specific applications.*

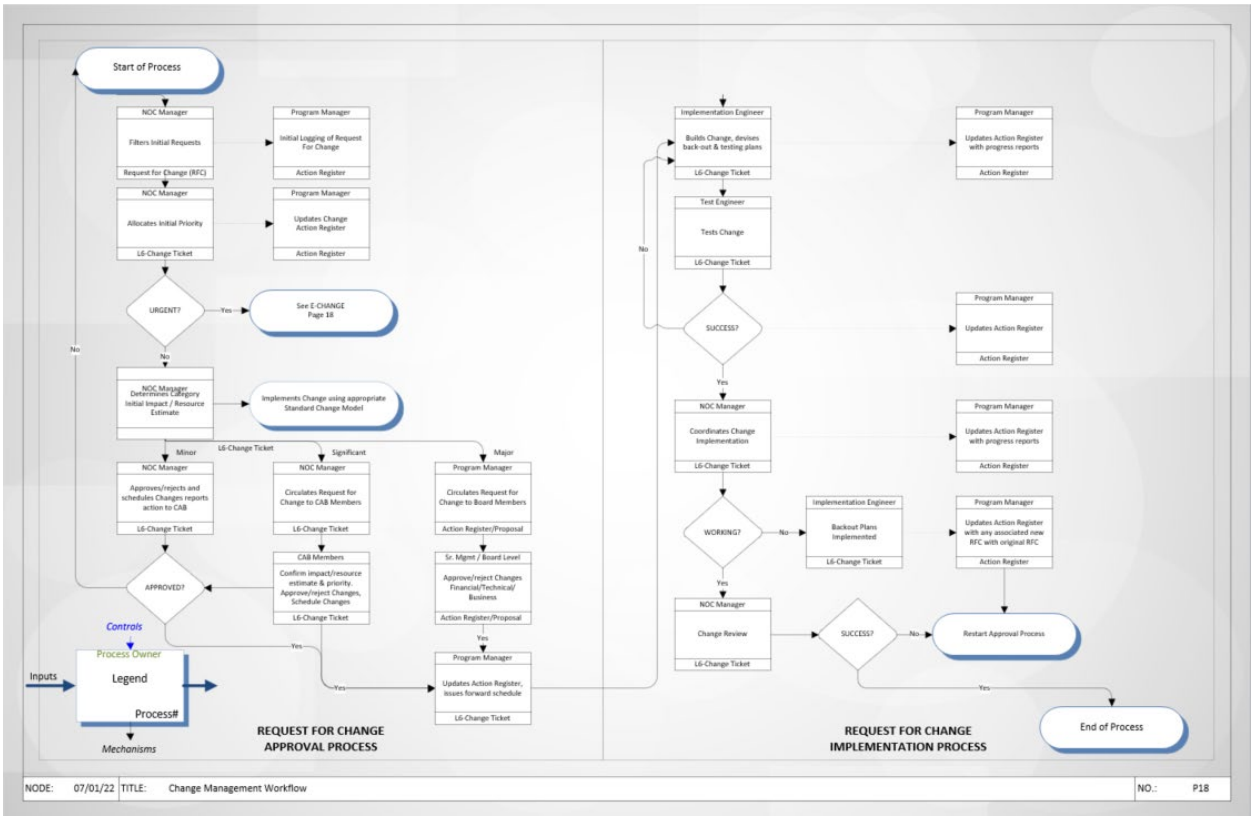



*Figure 14: Change Management Workflow*

## Level 2 Engineer Roles & Responsibilities

| L2 | Second Level Engineer / REMEDIATE | |
|---|---|---|
| Role  | **L2 Engineer** will discover, diagnose, restore, remediate the Incident by Knowledge Base Articles, Work Instructions or Professional Expertise. L2 Engineers are responsible for developing Knowledge Base Articles for L1 Analysts. L2 Engineers are responsible for Configuration Items within the Service Center including alert configurations, notification rules, site groups, service groups and policy modules. The role of a L2 Engineer is to return the device to steady-state operations and maintain configuration settings for the Monitoring Environment. | |
| Escalation Policy | If the L2 Engineer cannot resolve the Incident within the parameters specified, the L2 Engineer will escalate / notify the appropriate staff within the Service Manual Procedures. Based on the defined procedures, the L2 Engineer may escalate a L3 Subject Matter Expert/Technical Architect for the device. That SME may be at the Provider, the Client, or Third-Party as determined by the Rules of Engagement. | |
| Skill | **Industry Certifications:** Microsoft MCP, MCTS Exchange; Cisco CCNA (Security, Wireless, Networking) | |
| RACI | **Investigate Alert:** Research Frequency of Incident against Alert History | |
| | **Diagnose Incident:** Research Incident against Known Errors/Resolutions | |
| | **Document Resolution:** Produce Knowledge Base Article for Future Remediation | |
| | **Outcomes:** Remediate, Restore, Evaluate, Escalate | |
| SLO / SLA | **Mean Time to Resolve (MTTR):** Objective: < 1 Hr; Threshold 2 Hrs; | |

## Service Level Management

| | **Mean Time to Resolution (MTTR) Time Based on Priority for 90% of Incidents** | | | |
|---|---|---|---|---|
| Premium | P1: Urgent | P2: High | P3: Normal | P4: Low |
| Service | 1 hour | 2 hours | 8 hours | 24 hours |

| | **Mean Time to Resolution (MTTR) Time Based on Problem Management Investigation** | | | |
|---|---|---|---|---|
| Premium | STR24 hours | STR48 hours | STR7 Days | STR14 Days |
| Service | 60% | 70% | 80% | 90% |

| | **Mean Time to Resolution (MTTR) Time Based on Change Management Implementation** | | | |
|---|---|---|---|---|
| Premium | STR24 hours | STR48 hours | STR7 Days | STR14 Days |
| Service | 60% | 70% | 80% | 90% |

| | **Mean Time to Resolution (MTTR) Time Based on Request Management Fulfillment** | | | |
|---|---|---|---|---|
| Premium | STR24 hours | STR48 hours | STR7 Days | STR14 Days |
| Service | 60% | 70% | 80% | 90% |

- **P1: Urgent** - An emergency condition that prevents critical business operations.
- **P2: High** - A condition that significantly impairs the use of one or more applications or systems to perform any critical business operations.
- **P3: Normal** - One or more applications or systems are affected, but the impact on business operations is not severe.
- **P4: Low** - The reported issue does not substantially impact business operations.

# Level 3: Resolve

## Capacity & Performance Management

In addition to the services offered in **Respond** and **Remediate**, the **Resolve** service offers utilization analysis to provide capacity planning for the managed site(s). This level is only available with the premium, an on-shore, US-based NOC service. With the **Resolve** service, you receive:

- All benefits of **Respond** and **Remediate**
- Root cause analysis, problem reporting, and error frequency analysis
- Performance data gathering and analysis for capacity planning
- Maintain logs, data, and statistics for customer review

## Standardized Processes

### Capacity Management:

Capacity management refers to the act of ensuring a business maximizes its potential activities and production output—at all times, under all conditions. The capacity of a business measures how much companies can achieve, produce, or sell within a given time period.

The Capacity Manager is responsible for ensuring that services and infrastructure are able to deliver the agreed capacity and performance targets in a cost effective and timely manner. He considers all resources required to deliver the service, and plans for short-, medium- and long-term business requirements.

- The right infrastructure and service designs to address business needs
- The right processes in place that can be implemented with minimal interruption
- The right number of resources (workstations, servers, supplies) to meet deadlines and production quotas
- The right people with the ability to do the necessary work to meet service level agreements
- The right amount of budget allocated for optimal efficiency at a minimal price
- The capacity to problem solves and respond quickly to meet current and future needs

### Performance Management:

Performance management is the practice of managing network service response time, consistency, and quality for individual and overall services. Maintenance usage data, statistics, and logs for utilization analysis
Observe error frequencies, analyze utilization, and conduct capacity planning

## Level 3 Subject Matter Expert Roles & Responsibilities

| L3 | Third Level Escalation - Subject Matter Expert / RESOLVE | |
|---|---|---|
| Role  | **Level 3** Subject Matter Expert is brought into the incident to assess the situation, and work with all stakeholders to remediate and restore service to a steady state operation. The NOC will capture the incident information, document processes and procedures for managing this activity during the implementation phase. Tickets related to major outages will be collected into one master ticket and counted as a single problem.<br><br>A major outage is defined as the failure of an End Component that has a significant technical and business impact on the customer's operations, is not documented in standard operating procedures for restoration of service, or an incident that extends beyond 2 hours in total duration. | |
| Additional Roles | Level 3 Subject Matter Expert may also be an outsourced resource for Patch Services, Active Directory Administration & Proactive Engineering Activities. Level 3 Subject Matter Expert is the primary resource for new service design and system architecture. Their engagement level for Incident Management is to be Consulted as a matter of technical reference. | |
| Skill | **Industry Certifications:** Microsoft MCSE/MCSA, Cisco CCNP (Security, Wireless, Networking), VMware VCP | |
| RACI | **Isolate Incident:** Establish Root Cause Analysis | |
| | Provide Workaround: Full Resolution | |
| | **Document Incident:** Create Knowledge Base Article | |
| | **Outcomes:** Restore, Restart, Remediate, Repair, Reconfigure, Rearchitect | |
| SLO / SLA | **P1: Mean Time to Resolve (MTTR):** Objective: < 2 Hrs; Threshold 4 Hrs; | |
| | **P2: Mean Time to Resolve (MTTR):** Objective: < 4 Hrs; Threshold 8 Hrs; | |

## Service Level Management

| | **Mean Time to Resolution (MTTR) Time Based on Priority for 90% of Incidents** | | | |
|---|---|---|---|---|
| Premium | P1: Urgent | P2: High | P3: Normal | P4: Low |
| Service | 1 hour | 2 hours | 8 hours | 24 hours |

- **P1: Urgent** - An emergency condition that prevents critical business operations.
- **P2: High** - A condition that significantly impairs the use of one or more applications or systems to perform any critical business operations.
- **P3: Normal** - One or more applications or systems are affected, but the impact on business operations is not severe.
- **P4: Low** - The reported issue does not substantially impact business operations.

## Level 2+: Service Level Management

Service Level Management (SLM) is one of five components in the ITIL Service Delivery area. It is arguably the most important set of processes within the ITIL framework. SLM processes provide a framework by which services are defined, service levels required to support business processes are agreed upon, Service Level Agreements (SLAs) and Operational Level Agreements (OLAs) are developed to satisfy the agreements, and costs of services are developed.

In the end, business units are justifying to senior management the levels of service needed to support business processes, not IT. And the built-in continuous improvement processes ensure that when business needs change, supporting IT services change with them.

### Reporting:

- Weekly activity summary including open incident tickets, closed incident tickets, automated activities performed, and remote sessions conducted
  - MWNOC – Daily Activity Report
  - MWNOC – Device Spec Report
  - MWNOC – Trouble Ticket Details
- Monthly activity summary including open incident tickets, incident tickets open for more than one day, closed incident tickets, automated sessions conducted, and graph summarizing monthly activity
  - MWNOC – Monthly Activity Summary
  - MWNOC – Site Monthly Executive Report
  - Software Patch Compliance Report

| L2+ | IT Service Management / REPORT | Jointly Provided |
|---|---|---|
| **Role**  | **L2+ Service Management** will add the Reporting & Documentation Services for the production of automated reports that will be published by the Service Center. The Service Center is the source for Ticket Activity and Site Reporting. | |
| **Deliverables** | **Weekly/Monthly Reports** will be published in the Service Center to document the Health/Performance of the Customer's Network. Within the Weekly Reports are Service Level Snapshots (PDF) of the Daily Dashboard. | |
| | **IT Glue Runbook** the full runbook of activities is the accumulation of Knowledge Management for each client. Runbooks can be generated upon request. | |
| | **Client Business Reviews** are the responsibility of the MSP and how to best invest your IT budget and control costs. | |
| | | |
| **Skill** | **Business Management & IT Executive Analysis** | |
| **RACI** | **Provide Reporting:** Weekly/Monthly Reports including Executive Summary, Work Completed, Hardware/Software Inventory, Site Business Report | |
| | **Provide Reporting:** Monthly/Quarterly Client Business Reviews | |
| **SLO / SLA** | **Daily Reports:** Past Business Day activities extracted, transformed, loaded into analytics tool and posted in Customer Portal. | |
| | **Weekly Reports:** Distributed Monday 12:00AM, posted in Customer Portal Monday 12:00PM | |
| | **Monthly Reports:** Distributed Last Day of Month 12:00 AM, posted in Customer Portal First Day of Next Month 12:00PM | |
| | **Client Business Reviews:** Scheduled Second Business Week of the Month | |

# NOC Services Features Overview:

| NOCDOC NOC Services Feature List | Level 1 Respond<br><br>Monitoring & Event Management | Level 2 Remediate<br><br>Incident Management | Level 3 Resolve<br><br>Capacity & Performance Management |
|---|---|---|---|
| 24x7 Monitoring & Verification | ✓ | ✓ | ✓ |
| NOCDOC RMM Monitoring | ✓ | ✓ | ✓ |
| Inventory and asset management | ✓ | ✓ | ✓ |
| Auto-discovery of new devices | ✓ | ✓ | ✓ |
| Ticketing & Workflow | ✓ | ✓ | ✓ |
| Critical Service Monitoring | ✓ | ✓ | ✓ |
| Server Monitoring | ✓ | ✓ | ✓ |
| Backup Monitoring | ✓ | ✓ | ✓ |
| Antivirus Monitoring | ✓ | ✓ | ✓ |
| Suggested troubleshooting tips | ✓ | ✓ | ✓ |
| Escalation and notifications | ✓ | ✓ | ✓ |
| MWNOC Automated Reporting | ✓ | ✓ | ✓ |
| Incident Management | | ✓ | ✓ |
| Microsoft OS Patch Management – Critical and Security | | ✓ | ✓ |
| Network Management | | ✓ | ✓ |
| Messaging Management | | ✓ | ✓ |
| Storage Management | | ✓ | ✓ |
| VMware Administration | | ✓ | ✓ |
| Automation of Maintenance Tasks | | ✓ | ✓ |
| Provisioning, initialization, and restoration of device(s) | | ✓ | ✓ |
| Maintenance Reboots | | ✓ | ✓ |
| Change Management | | ✓ | ✓ |
| Software Distribution | | ✓ | ✓ |
| Backup Management | | ✓ | ✓ |
| Antivirus Management | | ✓ | ✓ |
| Error Frequency & Pattern Recognition | | ✓ | ✓ |
| Problem Management | | ✓ | ✓ |
| Root Cause Analysis | | ✓ | ✓ |
| Utilization Analysis | | | ✓ |
| Capacity Planning | | | ✓ |
| Maintain logs, data, and statistics | | | ✓ |
| Data Analysis | | | ✓ |

# Service Desk (SDX) Overview:

NOCDOC's Service Desk offering allows the MSP to extend their capacity with 24x7 support for customers without increasing the team or having an overnight paging service. The Service Desk Service provides support services directly to the end users of your customers through a branded ticketing portal.

Service Desk Management has the purpose to provide a Single Point of Contact for End-User Computing Issues when there is a disruption of service, for service requests, or even for some categories of request for change. The Service Desk provides a point of communication to the users and a point of coordination for several IT groups and processes. The Service Desk team will address all end user questions such as their password recovery, common computer (Microsoft suite) programs, and network access issues.

## Access via Email / Chat / Web / Phone

Four channels of communication for support to include Unique Inbound Phone number, Chat, Email, and Web Form for support. MSP's can forward from their existing support line to the Unique Inbound Phone Number.

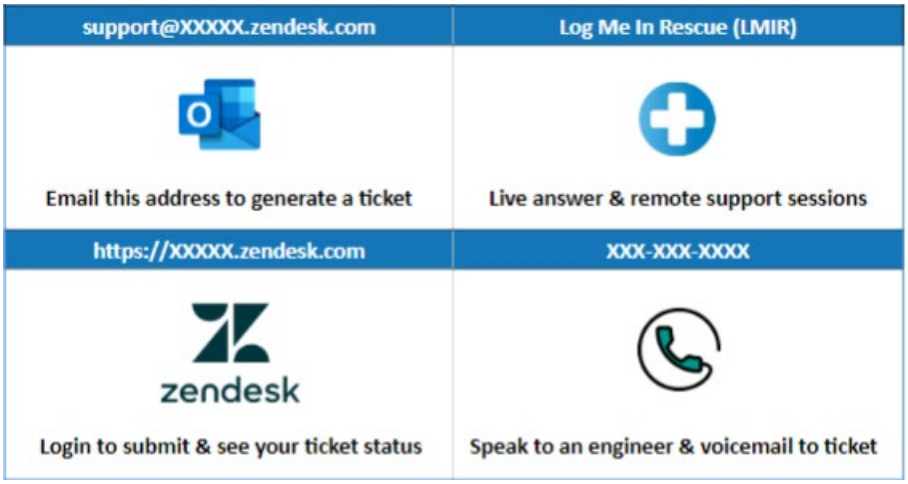



*Figure 15: Service Desk Methods of Contact*

## Branding & Integration

Most MSP's have a Professional Services Automation (PSA) system from which the team works everyday. To add licensing for the NOCDOC NOC/SDX (50+ Analysts, Engineers, SME's) is not economically smart for either party. As a result, we will create a spoke from our https://nocdoc.zendesk.com hub that can be custom branded for the MSP. The external facing part of the IT Service Management system will have the MSP's branding and email communications to maintain the MSP's identity and brand.

On the internal support side of Zendesk, we can take advantage of standardized process, macro customizations and 10+ year of application add-ins. The outcome is that standardized templates allow the Onboarding Team to stand-up new Zendesk instances in a few days. This enables our Onboarding team to create API based integrations with the MSP's existing PSA>

## Knowledgebase Management

Core infrastructure Knowledge Management will be in IT Glue under the client's organization. Relevant end-user support information is a cataloged in the Zendesk Guide (Knowledgebase) for Point of Use and security purposes.

Included in NOCDOC Service Desk Service are:

| PC and Mac Workstations | Service Description |
|---|---|
| Operating system support | Assist users with system and application error messages, enabling or removing start-up programs, removing programs, enabling and scheduling performance optimization and maintenance features, managing attached devices such as printers and scanners. |
| Hardware and driver support | Perform remote diagnostics and root cause analysis for malfunctions with computer hardware components, including assistance recovery and installation of the most current drivers for the end user's hardware. |
| Web application support | Assist end users with general business applications such as Microsoft Internet Explorer, Microsoft Outlook, and other web applications. |
| Security | Installation and operation of antivirus, antispam and firewalls. Assistance in the diagnosis, control, and removal of infections using NOCDOC RMM remote automated tools. |
| Software Installation | Technical support for the installation and operation of commercial application software applications, in accordance with manufacturer's specifications and provisions. |
| Mobile devices | Technical support for connectivity and collaboration between PC and digital devices such as Apple iOS, Windows Mobile, and Android |
| LAN Connectivity | Assistance in configuring and troubleshooting registered computers to participate in a local area network (LAN), wired or wireless for file and device sharing, such as shared printers, disk drives, external storage, scanners, and multimedia equipment, as well as internet access. |
| General support | Thorough understanding of end user issues through screen sharing, chat, and phone, as well as to illustrate and execute appropriate solutions effectively and efficiently |

## Service, Details & Execution (SDX):

The NOCDOC Service Desk offering focuses on three areas to deliver end-user support.

### Service

#### *Acknowledgement and Ticket Initiation*

- "Be Quick to Answer, it is an opportunity to Serve"
- Remember to be cordial and engaged when working with customers over the phone and in remote sessions
- Ask 2 Critically thought-out questions to gather more information to put into Public Comments for a received incident or request fulfillment
- Assign

#### *Etiquette*

- Communication is essential throughout the life of the ticket for great customer service and high-level execution
- For security and data privacy verify who you are working with is listed in the system and if not follow proper security processes
- Use comments to keep the user, partner and your team informed of progress and next steps
- Use the customers first name and include device names when gathering details in the ticket avoid referring to the customer, the device or server without being specific in your ticket notes
- Our responsibility is to follow up until we have resolved the incident or task by placing public comments of next steps or that the investigation is ongoing after internal notes

- Set expectations and provide public comments to let the customer know that their issue is still being investigated or worked on
- Be mindful of how long you have been on the phone, in a session and or the age of a ticket to ensure that you are using your time and the customers time wisely
- Set appointments that work for the user and yourself and then ensure that appointment is kept

## Details

### *30-minute R.I.D.E*

- **Review** the event received from the user and determine whether or not it is an incident or a task
- **Investigate** the incident or task without making assumptions while troubleshooting and look for any knowledgebase articles and or white papers that may be of assistance
- **Document** what was reviewed with the user and all steps taken during the investigation
- **Execute** a plan for resolution developed from the review, investigation and all documented notes while working with the user

### *Tickets*

- Event management is determining when a new ticket is received whether it is an Incident vs Task and the priority
- Screenshots paint a clearer picture that words cannot which is crucial when reviewing an incident or configuration setup
- Before executing a plan for resolution make sure you have a rollback plan and aren't making changes that will leave the user without at least a temporary workaround
- Tasks should be scheduled and can be a part of a project but no matter what should always have a confirmed completion date and defined requirements
- Incidents can affect the user or the device so validating both the user's information and gathering the devices information specifically name and specs are equally important

### *Troubleshooting*

- Do not assume you will resolve the event if you have not validated what the event is first
- Remember to "get back to the basics" even though issues may seem complex or we may have never encountered the event always start by asking questions
- Don't look for just the symptoms otherwise the root of those symptoms could be missed and there could more than one root. Review, investigate and document before executing a solution
- Think of who, what, when where, why and how in a general sense as answering all of those may not be possible but remember they may also be causing the symptoms as well
- Have mental Check Points of how much time you have spent working on the incident/task and how much time it would take to resolve in an efficient manner

### *Internal Review Team*

- Collaborate with Internal Review team through proper channels after validation, troubleshooting and 30-minute R.I.D.E
- Ensure ticket notes contain an internal note "Collaborating with the Internal Review team"
- Internal Review team can audit articles used and provide instruction for new knowledge articles and SOP additions to database

- Internal Review team will collaborate and coordinate with the engineer next steps and place a tag in the ticket review has taken place prior to partner/vendor knowledge transfer-escalation
- Internal Review can provide knowledge transfer, troubleshooting steps and define a path for partner/vendor knowledge transfer-escalation or dispatch

*Partner/Vendor KT-E (Knowledge Transfer-Escalation)*

- Troubleshooting is required prior to escalation even if there is no SOP or knowledge of the app/system. To validate the need for escalation you must first troubleshoot the event
- If immediate escalation is designated by an SOP, we must first validate the event meets the requirements for immediate escalation and then call the partner/vendor for a warm handoff
- At times there are distribution groups, automations and or configuration items that are required for escalation to the partner/vendor make sure these are implemented prior to escalation
- Not all contact with the partner/vendor will be an escalation. After collaboration with the Internal Review team place a call to the partner/vendor for knowledge transfer on articles
- Always gather the name and all details of the conversation when working with the Partner/Vendor including a case number if provided to place in your notes

## Execution

*Green Team*

- Responsible for all new (Green) ticket events that arrive on the board during allotted time. These tickets will be worked on but do not have to be completed during this time
- Status on the phone and in remote tools will reflect the engineer working through allotted Green Team time to focus on all new events. Ex. Green Team status on phone and Away in LMIR
- Each engineer Green team time helps maintain high availability and high ASR for our customers by focusing on all new tickets that are received through email and web form
- During this time critically thought-out questions will be asked to determine incident vs task and priority within the ticket and or over the phone

*Open-Backlog*

- During this time throughout the day engineers are responsible for making outgoing calls on open tickets, backlog tickets and or scheduled appointments
- Receiving incoming calls if available or delegated by manager
- Engineers are required to be logged into the phone system at the start of their shift and their status on the phone or LMIR will reflect their activity Ex. Green Team, Voicemail, Outgoing, etc.
- An open ticket status cannot be changed to pending or on hold without a comment containing next steps, a phone call and voicemail made, or setting an appointment
- For project work after approved by their manager engineers can use the designated Open-Backlog time to work on the project tasks
- Time can be allotted for continuing education and review to create new knowledge articles or meet with the Internal Review Team on open and backlog tickets

*Voicemail-Available*

- Voicemail sessions are an hour long and engineers are to be in a status of idle on their phone and available to take a call. LMIR status should be available as well during this time

- When a voicemail is received while the engineer is on the phone during this time they can change their phone status to Voicemail to listen and review voicemails received
- Engineers are responsible for creating and working voicemail tickets received and immediate callbacks should be made on all high priority voicemails
- Voicemails could arrive in different mailboxes or distribution groups and after listening should have a ticket created for the user that left the voicemail
- When voicemails are not received engineers are responsible for any tickets that are assigned to them that are more than 24-48 hours' old and need to be brought to the Internal Review team
- If when closing on the end of a voicemail session a large number of voicemails come in the engineer should ask for help from the next person on voicemail time and or an L3 engineer to help create tickets and call the users back

### *Red Zone*

- Incident tickets that are in the following state: in a status of open, are in the L2 assignee group and have not been resolved in 24 hours will appear as red on the dashboard
- Red Zone will let each engineer know what L2 incident tickets they need a follow up with the user on, continue troubleshooting and or need to collaborate with the Internal Review team
- The Red Zone is a visual representation of when our speed to resolve L2 incidents in 24 hours is missed and will help drive strategies and set goals to increase our L2 incident STR 2,4,8 and 24
- The Red Zone should increase the quantity of outgoing calls, appointments, follow ups and instill a sense of urgency for L2 incident resolution for each engineer
- Using the 30-minute R.I.D.E, detailed troubleshooting, available-open times, voicemail-backlog times, and collaboration each engineers Red Zone should gradually decrease and STR increase

## Service Level Agreement

| | **Average Speed to Respond (ASR) Time** | | | |
|---|---|---|---|---|
| Premium | Phone | Chat | Email | Website |
| Service | 30 seconds | 30 seconds | 30 minutes | 30 minutes |
| (VIP Users) | 30 seconds | 30 seconds | 15 minutes | 15 minutes |

- **P1: Urgent** - An emergency condition that prevents critical business operations.
- **P2: High** - A condition that significantly impairs the use of one or more applications or systems to perform any critical business operations.
- **P3: Normal** - One or more applications or systems are affected, but the impact on business operations is not severe.
- **P4: Low** - The reported issue does not substantially impact business operations.

| | **Mean Time to Resolution (MTTR) Time Based on Level of Incidents** | | | |
|---|---|---|---|---|
| Premium | Level 1 | Level 2 | Level 3 | Level 4 |
| Service | <2 Hours | <4 Hours | <8 Hours | <24 hours |
| | 60% | 70% | 80% | 90% |

| | **Mean Time to Resolution (MTTR) Time Based on Request Management Fulfillment** | | | |
|---|---|---|---|---|
| Premium | STR24 hours | STR48 hours | STR7 Days | STR14 Days |
| Service | 60% | 70% | 80% | 90% |

# NOCDOC Security Operations Center

## Introduction

The CIS Controls® are a prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks. They are developed by a community of information technology (IT) experts who apply their first-hand experience as cyber defenders to create these globally accepted security best practices. The experts who develop the CIS Controls come from a wide range of sectors including retail, manufacturing, healthcare, education, government, defense, and others. While the CIS Controls address the general practices that most organizations should take to secure their systems, some operational environments may present unique requirements not addressed by the CIS Controls. NOCDOC uses this framework in our Service Operations Center as we look at how to secure your business.




*Figure 16: CIS Control Graphics*

The security challenges facing the usage of technology in the enterprise warrant vigilance and a defense in depth approach to allow organizations to maintain confidentiality of their assets and information, availability of systems that support the business, integrity of information and data security. Our goal is to align our services and technologies to address the above goals.




*Figure 17: C.I.A. Graphic*

## 01 – Inventory and Control of Enterprise Assets

**Overview** - Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/ Internet of Things (IoT) devices; and servers) connected to the infrastructure, physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.

**Objective** - Hardware inventories are important for any device accessing the enterprise network. Our goal in to monitor, manage, analyze, and optimize infrastructure assets that are in scope for us to faults, failures, configuration, accounting, performance, and security related issues. Scope of work that is included in these services is to deploy our monitoring tools, look for faults and failures generated by alerts from the systems, monitor, manage and patch selected devices for compliance. For mobile devices, MDM tools can be deployed to support this process where appropriate.

**Technologies** –We will leverage Remote Monitoring and Management platforms to monitor, manage, patch, and remediate selected equipment inventory authorized by the client. The platform allows us to monitor anomalies of systems and provides our engineers the ability to quickly access the device based upon permissions and remediate issues that arise. Additional tools can be deployed for Mobile Device Management, Apple devices, and advanced network analysis if we need additional monitoring.

## 02 – Inventory and Control of Software Assets

**Overview** - Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

**Objective** – Software assets to be tracked and maintained to include firmware, OS, and common off the shelf – COTS applications as well as third party application if needed. The purpose is to maintain an inventory of licensed software installed on enterprise assets and periodically review software inventory to ensure it is up to date and accounted for. Ensure that support software is authorized for use in the enterprise and unauthorized software is removed.

**Technologies -** We will leverage Remote Monitoring and Management platforms to monitor, manage, patch, and remediate selected equipment software inventory authorized by the client. The platform allows us to patch and update system software and provides our engineers the ability to quickly access the device based upon permissions and remediate issues that arise. Additional tools can be deployed for third party applications, Mobile Device Management, Apple devices, and advanced network analysis if we need additional monitoring.

---

## 03 – Data Protection

**Overview** - Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

**Objective –** Remote access to your systems for outside users and partners is vital for today's business, but also a fertile avenue for attacks from cyber criminals. The goal for this control is to establish and maintain data management, data inventory, enforce data retention, encrypt data on end user devices, and deploy data loss prevention technology to control the movement of data coming and going.

**Technologies –** We will deploy technologies that will protect, control and prevent data leaks, monitor user activity, monitor for unknown applications, storage control, insider threats, as well as provide real time alerts. The technologies we use can provide ringfencing of the data as well as applications to prevent unwanted access to said applications and data.

---

## 04 - Secure Configuration of Enterprise Assets and Software

**Overview** - Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).

**Objective –** To provide a checks and balance roles-based approach to maintain and manage enterprise assets, manage firewalls, manage default accounts, enforce remote wipe capabilities for mobile assets, and configure assets with group policies that are aligned to corporate objectives for control of assets and software.

**Technologies –** Our engineer staff and systems use roles-based access to equipment that allows a good check and balance to monitoring and managing corporate assets. Our level 1 analysts can interact with the equipment once alerts are generated while our level 2 engineers have the ability to remediate and manage assets in accordance with corporate guidelines. Our monitoring and management platforms will monitor who has accessed assets and controls.

## 05 – Account Management

**Overview** – Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.

**Objective** – The goal of this objective is to establish and maintain an inventory of accounts, provide unique and secure passwords to systems, disable dormant accounts, and restrict administrator privileges to select accounts.

**Technologies** – Our team utilized a secure documentation platform that retains each clients sensitive data and documentation in a common portal that allows all stakeholders who need to have access, access the information when needed. In addition, the technologies we use allow the stakeholders to create runbooks and offline documentation for audits and attestations when needed. All documentation is structured offering an optimal way for organizing the information to effectively service the team. Access to documentation is controlled through account management and multi-factor authentication processes.

## 06 – Access Control Management

**Overview** – Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.

**Objective** – Establish an access granting process, revoking process, MFA for externally exposed applications, and centralized access controls.

**Technologies** – When using our team for service operations, you are creating a system of checks and balances where we look for two-man control to allow access for granting permissions based upon roles. Our platforms are all based upon roles base usage controlling and directing the work to the person who is authorized to perform the service. Using our service desk allows the end user to submit request to onboard and offboard staff as well as to provide and revoke permissions when needed to appropriate systems. In addition, our team can deploy technologies that support multifactor authentication to verify identity in seconds while at the same time protecting applications. In today's world it is imperative to use unique passwords and monitor exposure and use of those passwords in real time. Technologies can be deployed to assist the users in password management and single sign on.

## 07 – Continuous Vulnerability Management

**Overview** – Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure to remediate and minimize the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.

**Objective** – The goal of this control is to establish and maintain a vulnerability management process for patching, maintaining a remediation process for operating systems and common off the shelf applications. Remediate detected vulnerabilities as they arise.

**Technologies** – Our monitoring and management platforms have the ability for our team to deploy patches and updates to the operating systems, and COT's software via a management console that allows the team to schedule and maintain control of vulnerabilities for key systems and end points.

Deployment of our SOC as a Service that can leverage a threat monitoring platform to detect malicious and suspicious activity across the three attack vectors: Endpoint, Network, and Cloud. Our engineers and technology deployed will hunt and investigate threat activity across your systems and perform triage of detections and work with our NOC to remediate when actionable threats are discovered.

---

## 08 – Audit Log Management - SOC

**Overview** – Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.

**Objective** – To collect, maintain and retain audit logs for key systems. To Analyze and provide a Security Operations Center (SOC) as a Service in looking for vulnerabilities in the organization.

**Technologies** – Our engineers will review your logging process and discuss your retention requirements for enterprise assets. We can deploy technologies and a managed monitoring service to collect and analyze logs from key systems looking for vulnerabilities with our SIEM platforms and service.

Deployment of our SOC as a Service will leverage a threat monitoring platform to detect malicious and suspicious activity across the three attack vectors: Endpoint, Network, and Cloud. Our engineers and technology will hunt and investigate threat activity across your systems and perform triage of detections and work with our NOC to remediate when actionable threats are discovered. We have the ability to deploy cloud-based protection services for applications such as Microsoft 365, G Suite, Azure, AWS, Dropbox and more.

Additional services can include incident response planning, incident response, phishing simulations, as well as forensic services.

---

## 09 – Email and Web Brower Protection

**Overview** – Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement. 86% of all corporate attacks originate through someone's access to email or the web accessing something that originates as the beginnings of a malware attack.

**Objective** – Ensure the use of only fully supported browsers and email applications, Use of DNS filtering, restriction of unnecessary or unauthorized email or web browser, Implementation of DMARC and deployment of email server anti-malware protections such as scanning and sandboxing. In addition, look for suspicious activity of dark web for email domains.

**Technologies** – Our team can deploy technologies that are intended to protect your web browser and emails from malware and spam, as well as advanced threat protection. In addition we can use AI technologies to protect from Phishing and business email compromise, account takeover, domain fraud and DNS filtering. Our dark web monitoring technology helps protect businesses from cybersecurity incidents due to compromised credentials. Our team monitors the dark web in real time and our systems will issue alerts whenever exposed credentials are found, ensuring end users are notified and defensive measure can be taken before a breach occurs.

---

## 10 – Malware Defense

**Overview** – Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets. In today's hybrid work world, the worker is in the office behind the firewall and then working from home.

**Objective** – We need to provide technologies and services that will constantly protect the user and corporate no matter where they sit. To deploy technologies that will maintain anti – malware software on enterprise assets, Data execution prevention, and actively monitor assets for threats.

**Technologies** – Most people think of malware defense is deployment of an anti-virus tool. In today's world is a combination of anti-virus and anti-malware along with zero trust technologies that are deployed to protect corporate assets. Our MDR – Managed Detection and Response and XDR Extended Detection and Response device protection services are backed by a team of 24X7 threat hunters working with our SOC and NOC team to find and remediate real time footholds and threats as they happen. The AI platform looks for persistent footholds and malware and alerts our team with an action plan to remediate the threat called process insights. Used in conjunction with our SOCaaS platform we look for real time threats and work together to remediate those threats as they occur.

## 11 – Data Recovery

**Overview** – Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.

**Objective** – To develop and maintain a data recovery process that will meet the clients RTO – Recovery Time Objectives for backups and return to normal operations. Perform automated backups of in scope enterprise assets as well as test data recovery against your RTO. The goal of the backup and recovery strategy is to mitigate the risk of lost systems due to equipment failure or ransomware attacks using good practices of site to cloud and high availability requirements for use of information to meet your RTO objective.

**Technologies** – Our team supports and provides backup technologies that will support your RTO from the end point to the data center. In addition, we utilize technologies that monitor changes in configuration files and store that information automatically in our online documentation platform. The technologies we deploy and use are in response to meet your business needs for high availability and recovery of information base upon the RTO of the organization.

## 12- Network Infrastructure Management

**Overview** – Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.

**Objective** – To ensure the network infrastructure is up to date, monitored and managed for availability, performance, and security

**Technologies** – We deploy technologies that allow our team to monitor, maintain, and manage the network as well as look for performance and documentation. In addition, we can deploy technologies that will allow us to create real time visualization documentation, IP Address management, Netflow, SFlow, and JFlow, as well as configuration backups and reporting (What we call Level 3 Analysis).

## 13- Network Monitoring and Defense

**Overview** – Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base

**Objective** – To centralize security event alerting, look for host-based intrusion detection, segmentation of network assets, collect network traffic flow logs, deploy host based intrusion detection solutions such as EDR – Endpoint Detection and Response, port level access control and application layer filtering.

**Technologies** - Our Network Operations Center senior engineers will work with the SOC and end user community to monitor and defend the network. We can deploy next generation firewalls, processes, and services to defend against security threat across the enterprise. We also can centralize the event alerting through our SOCaaS offering that collects the logs and analyzes the information looking for anomalies and behaviors that are not normal.

In addition, we can deploy technologies that will allow us to create real time visualization documentation, IP Address management, NetFlow, SFlow, and JFlow, as well as configuration backups and reporting (What we call Level 3 Analysis).

## 14 – Security Awareness and Skills Training

**Overview** – Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.

**Objective** – Train workforce to recognize social engineering attacks, authentication, data handling, password management, recognizing and reporting security incidents. Conduct security awareness training.

**Technologies** – We will deploy technologies that test the employees ability to click and respond to simulate training, continuous testing, and reporting for administrators as well as active incident response awareness.

## 15 – Service Provider Management

**Overview** – Develop a process to evaluate service providers who hold sensitive data or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.

**Objective** – Maintain and manage  an inventory of service providers, designate enterprise contacts for each provider on as needed basis, develop escalation procedures on when and where to use the provider.

**Technologies** – Our team works with over 80 services providers daily. Documentation for our network as well as the client network is maintained in our online documentation portal that has escalation procedures and processes of when and where to use service providers for each client.

## 16 – Application Software Security

**Overview** – Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.

**Objective** – Maintain a security application development process that addresses software vulnerabilities. Perform root cause analysis on software vulnerabilities. Maintain inventory of third-party software.

**Technologies** – Our team focuses on infrastructure monitoring, management and remediation and uses a few third-party partners that specialize in software development, systems development life cycle and software release management. We will engage our partners where needed to address these issues if requested.

## 17 – Incident Response Management

**Overview** – Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.

**Objective** – Identify persons to manage incidents, establish contact and escalation procedures, maintain process for reporting incidents, assign roles and responsibilities and conduct routine exercise for Incident Response.

**Technologies** – Our Service Operations Center has an incident response plan that addresses the business and technical response from identifying an incident, putting in an escalation and running and incident response with a business and technology response team working with the customer to restore operations to a steady state.

## 18 – Penetration Testing

**Overview** – Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.

**Objective** – Establish and maintain a penetration testing program, perform periodic test, remediate findings, and validate security measures

**Technologies** – While capable of performing the tests internally, we find it valuable to use our external partner network to conduct the tests to review processes and operations to validate security measures and remediate findings. Typically, these tests are run on an annual basis.