A Phased Approach
for Building a Next-Generation
Network Operations Center

A Planning Guide

By Shawn Ennis, CTO
Monolith Software
A Phased Approach for Building a Next-Generation Network Operations Center

Executive Summary

Why build your own network operations center? There are countless reasons that drive organizations to pursue such a strategy – to cope with growth through acquisition, to better manage costs and complexity, or for service providers, to drive revenue and deliver better service to customers.

This whitepaper, by Monolith Software, a leading provider of fault, availability, performance, service level management and dashboarding for service providers, network operations centers and large enterprises, has been written to provide CTOs, directors of operations and network operations managers with a handbook that guides them through a series of best practices for establishing, and then maturing toward the next generation operations center.

Why Build Your Own Network Operations Center?

There are many reasons why organizations consider establishing their own network operations center (NOC). These reasons vary based on the type of organization and focus of their business.

Some businesses view the NOC as an insurance policy, ensuring the prevention of downtime or critical outages that may impact the flow of business or revenue streams. Some establish a NOC as a way to drive down costs or drive revenue. And still others establish a NOC because they have reached a level of critical mass in technology investment, where it simply makes sense to centralize.

Many small, regional telecommunications companies may seek to realize cost advantages and economies of scale by banding together through the formation of a shared services network operations center. This shared-service NOC allows smaller telecommunications providers to offer their customers a level of service that goes beyond anything they could provide independently, while keeping respective costs low.

For service providers, such as an MSP, ISP or ASP, a NOC makes a great deal of business sense. This consolidated and centralized hub for management control can become yet another service capability to provide to customers. Rather than invest in a data center, hosting, and monitoring capabilities and staff, businesses turn to their service provider to manage this infrastructure on their behalf. This business model transforms the NOC – which is traditionally a cost center – into an engine for revenue growth and an area for unique competitive differentiation for a MSP/ISP/ASP.

Other organizations are driven to establish a NOC to better control their own destiny and costs. These businesses may have traditionally outsourced network management and monitoring services to a service provider, but for any number of reasons -- accelerated growth fuelled by acquisition, dissatisfaction with their outsourcer or the level of outages experienced, or strategic customer service level agreements -- may be at a point where it makes more economic and strategic sense for the business to embrace a "build versus buy" approach and bring the NOC in house.

Large enterprises operating on a global scale, providing services 24X7, 365 days a year, or operating to a follow the sun model, may also elect to establish their own NOC.

As complexity rises in the enterprise technical environment, the costs of managing and monitoring networks in a localized or distributed way simply become prohibitive. Enterprises that grow network monitoring capabilities incrementally or expand management coverage by way of acquisition; find themselves coping with overly complex management and monitoring environments made up of poorly integrated point tools. They frequently suffer from heavy resourcing burdens and duplication of effort. The best solution for the large enterprise is to wipe the slate clean with a consolidated and centralized NOC, serving the entire enterprise from a single point of control.

Regardless of your business motivation, once the decision has been taken within your organization to build a NOC, it is essential that you embark on a detailed planning effort to ensure you are building the right NOC for your business – one that reflects best practices in the industry, strikes the right level of maturity for your business, and lays the groundwork for you to construct a next generation network operations center that will serve today’s and tomorrow’s business needs.
Defining the Next Generation Network Operations Center

A next generation NOC represents the upper end of the maturity in operational management. It is an enabler and accelerator of business, and moves beyond reactive and curative mode to prevent and predict outages and failures. While the qualities of a next generation NOC are highly desirable in theory, they may just not be applicable to your business. Companies need to carefully examine the needs of their business, understand the effort required to reach the upper end of the maturity curve, and above all, be practical. Establishing a next generation NOC is not a feat accomplished in a short period of time and organizations should plan to walk before they run.

NOC Best Practices

Once the motivation to establish a NOC has been established, and the business is on board with the decision, it is critical that you invest time in proper planning before plunging into the design and implementation of a NOC.

NOC managers and directors of operations are encouraged – rather, urged – to factor into this planning process the best practices and planning considerations outlined in this paper, and carefully align the capabilities, scope and relative maturity level of their NOC to the needs of the business, so that the NOC is right-sized; and is built to succeed.

This planning phase will help focus your efforts and ensure you are making the right decisions on behalf of your business. It will also provide a much-needed rudder to guide this large-scale effort. NOC projects can very easily be overtaken by internal politics and over-zealous vendors, who can derail you from your goals.

Considerations in the planning phase include NOC organizational structure and tier model, NOC scope and service commitments, monitoring and management surveillance approach and tooling, and processes and procedures.

Establish Your Organizational Structure

One of the first considerations in your planning process is your NOC’s organizational structure. This structure will determine your specific resourcing needs and facility size. The structure you choose for your NOC is determined based on a number of factors:

- Total size of organization.
- Number of locations and time zones served.
- Customer expectations and service level commitments and agreements.
- Business service model – is service & support available 24X7 or 8X5?
- Is NOC support centralized or does it follow a follow the sun model?

Large-size NOCs typically adopt a tiered model within their organization. The level and complexity of the tiering model adopted, also depends on the factors outlined above. Below are common roles you find within a large, tiered NOC:

- NOC tier 1 represents the help desk, with support staff providing first line telephone support to customers – typically utilizing knowledgebase articles.
- NOC tier 2 engineers offer ‘next level up’ expertise for more complex problems. These engineers have access to vendor documentation, and are more senior, enabling them to engage in more in-depth troubleshooting on thorny customer issues.
A Phased Approach for Building a Next-Generation Network Operations Center

- NOC tier 3 engineers offer the most advanced level of customer support. Often known as the “tiger team,” tier 3 engineers are the most senior, have direct lines to vendors to advocate on behalf of customers, and provide custom, on-site engineering work.

- NOC shift supervisors and team leads have oversight for day to day staff management, policies, procedures and process. They make sure that no issue falls through the cracks and goes unattended.

- NOC directors typically have broader scope staffing responsibilities, including all NOC staff as well as field technicians.

- Vice president of IT or CTO is typically an active member of the management team, has accountability to the business, and has strategic authority over the NOC and technology direction, and its performance on behalf of the organization.

**Define Your NOC Policies and Procedures**

Does your organization have documented standard operating procedures, runbooks and a formal change management policy? Are you working in a regulated industry? Is there a requirement you support ISO 9000, or follow ITIL? Processes and procedures are a critical element to IT governance and to the operation of a network operations center, and should be defined prior to your build out of the NOC. A good place to begin is with existing process used by your teams today. This provides a starting point and a baseline for incremental improvement and greater maturity over time.

Probably the most critical process to define within your NOC is your change process. It is a given that your business will change; your customers will change; and your environment and the configurations within that environment will change. This process should enable trouble ticketing, issue tracking, kick off escalation and approval cycles, provide for roll back of change if necessary and maintain thorough audit trails of every activity and resulting outcomes.

It is important when defining process, policy and procedures for your NOC that you not try to ‘boil the ocean.’ If you aim too high and design processes, procedures and associated metrics for performance that are beyond the capabilities of your organization, you create unattainable goals, and set your NOC and your team up for failure.

Better to start small by documenting the policies, processes and procedures used by your team today, and then automate process where possible by leveraging workflow within your selected monitoring platform. You can also leverage your monitoring platform’s knowledgebase to create articles that codify team knowledge and expertise.

**Align NOC Scope & Role to Business and Customer Expectations**

What are the expectations of the business for your network operations center, and are they in line with the relative maturity of the business, and your customer’s expectations? 99.999 availability and uptime is certainly an enviable goal, but a single configuration change can put this objective in jeopardy.

In establishing your next generation NOC, understand the objectives of the business, and align the NOCs scale and role to those objectives. Consider the following inputs when defining your NOC’s scope and establishing maturity goals:

- What is the acceptable outage window for your business? Is it hours, minutes or seconds?

- What impact will an outage have on the business in terms of lost revenue, customer satisfaction, or business reputation?

- What is your team’s average response time (mean time to respond or MTTR) when an outage occurs, and is there a goal to reduce this time window? And is that a reasonable goal? Keep in mind, MTTR is directly proportionate to the number of resources at your disposal. If you have more problems than you have bodies, your response time and recovery time will grow accordingly.

- What is your maintenance schedule, and what is your accepted window of maintenance downtime? Realize that routine maintenance is a part of the NOC existence. The environment will be forever changing. Technologies will be added and subtracted as capacity demands.
• Do you have service level agreements with customers that put additional conditions on the NOC, or place constraints on response and recovery times? What are the penalties and other risks associated with non-conformance to these SLAs?

If you carefully consider these factors, you should be able to construct a scope of service for your NOC that meets the needs of the business, offers an appropriate level of maturity, and will not jeopardize key customer relationships.

Select Your Management & Monitoring Environment
Now that you’ve decided on the shape and size of your organization, defined your policies, processes and procedures, and have right-sized the scope of responsibility for your NOC, it is time to equip your team for network surveillance, by selecting an appropriate management and monitoring platform. Depending on your point of origin, you may have some rudimentary management capability, such as open source tooling, or you may be reliant on a mix of point tools.

In either case, the creation of a next generation NOC gives you an ideal opportunity to institute a platform that is comprehensive, consolidated, seamlessly integrated, and future proof – capable of growing with the needs of your business as you evolve and change. In embarking upon tool and vendor selection here is some advice to consider:

• Define your request for proposal (RFP) based first upon the needs of the business, then upon operational concepts, and then finally upon technical functionality. Too often, RFPs become feature and function oriented, and selection teams become distracted by the latest vendor widget or dashboard display and lose sight of the problems they set out to solve in the first place. Consider vendors and technologies in the context of the business – is this investment making business sense? Will it help drive revenue? Can it help secure new customers? Will it allow you to cut costs?

• Look for a monitoring and management platform that gives you predictability. If you are able to comprehensively survey your network environment and anticipate problems before they occur, you are moving to a more evolved, next generation NOC, and can provide new strata of service to the business and to its customers.

• If you are a managed service provider, seriously consider monthly ‘by node’ pricing. It is likely that you are passing the costs of your management and monitoring services to your customers, charging customers per resource and per circuit. This pricing model will facilitate the generation of revenues for your business by possibly adding classes of monitoring services.

• Select a solution that is comprehensive, consolidated and future proof.

• Decide on your surveillance approach and stick to it. Are you going to be a map or dashboard-based NOC? Are you oriented around the helpdesk and a trouble ticketing system? Do you want to be event-based? The important thing to keep in mind is that in its early days, a NOC cannot be all things, and monitoring your environment in three or four different ways increases the complexity for your team and will more likely confuse than clarify – working directly against your stated goal.

Realize that your NOC environment is continually evolving as capacity shifts and new services are introduced. Your customers’ needs are also changing. Point tools in a NOC environment can force limitations that will actually prevent you and your team from becoming a next generation NOC.

Rather, seek out a solution that ideally is built on a single code base, can discover and incorporate a wide range of systems, applications, networks and devices, and that can easily evolve and incorporate tomorrow’s technologies.

Flexibility in a surveillance platform is critical. Regardless of the information requirement or your demand on the system, your management and monitoring platform should be capable of supporting that business need.
Key Qualities to Look for in a Next Generation Management and Monitoring Platform

The circumstances of your business will drive your tooling needs, but if you are seeking to build a next generation NOC over time, here are some qualities to look for in your surveillance platform:

- **Consolidated view** – multiple consoles confuse your staff and slow down the pace of business – counter to the goal of the next generation NOC. Look for a solution that offers you a single pane of glass view into your environment.

- **A single vendor solution** – a mosaic of disconnected point tools complicates the management effort, and multiple vendor relationships add additional costs and administrative burden to your team. If you are able to turn to a single vendor for all of your operational management requirements, you will simplify negotiations, lower maintenance costs, and streamline the vendor management process for your team.

- **Executive dashboards** – look for a solution that can support the information needs of executive team, as well as your NOC staff. This guarantees that information displayed has a high degree of reliability and accuracy. Dashboards should be real time, and draw information from the operations coal face – versus providing executives with a time-delayed and potentially biased interpretation of the facts.

- **Single code base** – a single, consolidated solution built on a unified code base will greatly reduce your administrative costs, shorten your implementation and training time, offer a lower total cost of ownership and generally make the monitoring effort simpler, even in the event of rising complexity in your customers’ environments.

Maturing Toward the Next Generation NOC

Now that you have established your NOC in accordance with the best practices we have outlined, it's time to look at the various maturity phases that you and your team may experience as you progress toward becoming a next generation NOC.

Again, with respect to process, it is important to take a phased approach to maturity of your NOC. Your team will be more successful, and your business will better adapt to an incremental approach to maturity. Taking a step by step approach also allows you to right size your NOC's maturity to the needs and growth trajectory of the business.

As we defined earlier in the paper, the next generation NOC represents the upper end of the maturity curve. NOCs at this level enable and accelerate business, and move beyond reactive and curative mode to prevent outages and failures. While the qualities of a next generation NOC are highly desirable in theory, they may just not be applicable to your business. Stopping at Phase 1 or Phase 2 may be exactly the right strategy for your organization.

**Phase 1 – The Reactive NOC**

Phase 1 of maturity covers the basic services that any NOC should be able to deliver on behalf of the business and customers it serves. Essentially the best litmus test to determine if you are operating your NOC at a Phase 1 level is to ask yourself: “How many outages have occurred in the past day, and what was the average length of each outage?”

If a network operations center is unable to answer these two questions, is unable to reactively respond in the face of an outage or failure, or does not know that the customer is suffering from an outage before they detect it, it is not yet working at a Phase 1 level of maturity.

That said, Phase 1 maturity presents a challenge for most organizations, and probably only about 5 percent of organizations fully conform to Phase 1 criteria. Here are the core services you should expect to see in a Phase 1 NOC:

- **Availability** – Your NOC should be capable of assuring that 100 percent of the production technology in the environment is up and running, informing customers in the event of an outage, and troubleshooting problems. Service level management and business service management may be methods for increasing productivity in this phase.
• **Ticketing** – Your NOC should be equipped with a trouble ticketing system that records all operational actions during an outage and facilitates post-mortem analysis of operational responses during a specific outage. Your ticketing system should also serve as the record of interaction with customers.

• **Reporting & dashboards** – Real time dashboards and accurate historical reporting provide a communication bridge between operations, executives and clients and enable availability reporting and post-mortem analysis and reporting.

**Phase 2 – The Proactive NOC**

If only 5 percent of organizations have fully reached Phase 1 of maturity, even fewer have reached Phase 2 where they are able to provide proactive network surveillance. A Phase 2 NOC builds on the basic services found in a Phase 1 NOC and is capable of finding and preventing problems before they become outages. The litmus test for determining if your NOC has achieved Phase 2 level of maturity is to ask yourself: “How many outages have we prevented today?”

Here are the core capabilities you should expect to see in a Phase 2 NOC:

• **Performance** – A Phase 2 NOC should be able to test that technology works within defined performance specifications and meets specifically defined thresholds, i.e. key performance indicators for bandwidth utilization and IO rates.

• **Fault, Auditing and Accounting** – Manual mis-configuration of network devices by trained employees is one of the leading causes of network outages. A Phase 2 NOC should be equipped to collect 100 percent of faults from devices, be able to pull audit logs from critical applications, and track the overall security of the network environment. Phase 2 NOCs should also have standard operating policies that ensure configuration changes are only performed during a pre-determined maintenance window and that all configurations are consistently and frequently backed up.

• **Operational performance monitoring** – A Phase 2 NOC should be able to plan, predict, track, then report upon their operational performance quality. Key metrics include the NOC’s ability to respond to issues, to recover from failure, and to provide appropriate benchmark data and trending to assist with post-mortem analysis, determine resourcing and engage in performance improvement.

• **Process management** – Standard operating procedures (SOPs) are expected within a Phase 2 NOC and are key instruments in ensuring the lowest amount of outages, in minimizing response times. SOPs also minimize the learning curve of your operators. They typically cover the full range of NOC procedures from incident management (as covered in a maturity framework such as ITIL) to something as simple as shift hand-off procedures. The better and more thorough the processes and policies of your NOC, the more predictable your operations will be.

**Phase 3 – Becoming the Experts**

The Phase 3 NOC has finally achieved the goal of becoming a next generation network operations center. This NOC is not only able to react to outages, and prevent outages from occurring; it is also capable of catching issues such as mis-configurations before they become problems. The litmus test to determine if your NOC has reached Phase 3 maturity, is to ask yourself the question: “How many outages and problems will you have tomorrow?” A Phase 3 NOC builds on Phases 1 and 2 and adds the additional capabilities:

• **Configuration management** – A Phase 3 NOC maintains complete control over all technology configurations in the network environment, knows when those configurations change, and can identify the reasons for those changes. Automatic pushes of configurations make the most of a scheduled maintenance outage. Peer reviews with testing and workflow-enabled approval cycles prevent the introduction of unwanted change and mis-configurations -- while tracking all activities associated with the change. Finally, roll back capabilities make it easy for change to be backed out if necessary.
A Phased Approach for Building a Next-Generation Network Operations Center

- **Capacity** – The majority of the firefighting efforts in a NOC originate due to a lack of capacity and prevention planning. A Phase 3 NOC should have the capability to perform detailed capacity planning, and have the ability to understand and project over- and under-capacity to appropriately align the NOC with the growth needs of the business. A Phase 3 NOC can also view its capacity in detailed terms – such as identifying bandwidth issues from latency issues – to ensure that customers are appropriately served.

- **Knowledgebase** – The expertise and intellectual capital of your NOC is critical to your business, and knowledge sharing can be the key to greater efficiency and productivity. A Phase 3 NOC will capture, document and disseminate knowledge so that issues can be resolved faster – ideally at the Tier 1 first line of defense. New employees are spun up faster and with fewer incidents when the collective knowledge of the NOC is at their fingertips.

- **Automatic remediation** – Within the Phase 3 NOC, common or frequently occurring issues and problems have well-defined processes, and solutions to these problems can be automated to increase productivity. This frees staff within the NOC to focus their energies on proactively attacking new and complex issues that arise within the network. The Phase 3 NOC will also employ capabilities such as enrichment and correlation to provide greater context around issues and reduce the event stream to probable causes.

**In Closing**

Creating a next generation NOC is not an easy task. It may not even be necessary for your business.

When establishing your NOC, it is critical that your organization plan before it acts, and leverage industry best practices such as those included in this whitepaper to establish NOC organizational structure, define scope, processes and procedures, and select a monitoring and management solution that will serve today and tomorrow’s needs.

Furthermore, it is important to know that maturity within the NOC is hard to achieve. It is estimated that only five percent of organizations have attained the first level of maturity allowing them to react and prevent outages.

To that end, NOC maturity should be viewed as a journey, taken one step at a time. Apply realistic goals that allow for a gradual ramp to maturity and progress through the various maturity phases. Start small, make consistent improvement, and don’t be afraid to settle on a level of maturity that serves your business best. Allow your customer’s expectations, the competitive landscape and the needs of your business drive the shape, size, and maturity level of your NOC.

**About the Author**

Shawn Ennis has spent his career utilizing management software to run Network Operations Centers, implementing management software solutions for a significant number of the largest service providers, enterprise companies, and government agencies in the United States, and developing management software solutions to meet the needs of client organizations.

Currently, Shawn Ennis is CTO and a Managing Partner of Monolith Software, a software company that delivers cost effective and highly scalable management solutions to organizations seeking to better manage their technology infrastructures. Shawn provides Monolith with leadership in company direction, technology, development, and Monolith’s support infrastructure.

Shawn brings real world experience and a deep understanding of NOC operations to the table for the customers Monolith serves. Operational management, technology development, and advanced enterprise management solutions have been key areas of focus throughout his career.