A Practical Guide to **Running an Effective NOC**

How to Build, Optimize, and Manage Your NOC to Maximize Performance and Uptime

INOC

NOC Lifecycle Solutions®

Table of Contents

AUTHOR BIO:

Ben Cone

SENIOR SOLUTIONS ENGINEER

Ben works with customers to understand their technical and operational support challenges and helps develop solutions to address their needs. He has managed numerous NOC onboarding projects for customers over the years and has an intimate understanding of infrastructure support issues. Before INOC, Ben developed data, voice, and related service offerings that included redundancy and security as the key features. Ben holds a Bachelor's in IT with a major in Computer Network Security Technology from Herzing University.

Introduction

No matter what kind of business you run, your IT infrastructure and applications are bound to be affected by outages. Every second of downtime can cost you time and money.

A properly built, well-managed Network Operations Center (NOC) not only mitigates these losses, but also improves network, infrastructure, and application performance. On the flip side, a poorly designed and managed NOC leaves your technology investments—and the business activities that rely on them—exposed and vulnerable.

This white paper reviews the purpose and functions of a NOC and covers the steps involved in designing, building, and managing a successful NOC. It also touches on the most common challenges NOCs face and shows how virtually all of them can be resolved or avoided by effectively operationalizing your NOC.

Whether you have an internal NOC or outsource this function, you'll come away with an understanding of how the NOC can deliver better value to your business and what it takes to get there.

The Purpose of a NOC

While the NOC's primary job is to maximize performance and uptime, it plays another crucial role that few organizations take full advantage of: minimizing the productivity loss to the business when IT assets go down for any reason.

Simply put, a high-functioning NOC does more than just keep your network, infrastructure, and applications up and running. It can quickly inform impacted users of a problem, enabling them to shift their attention to other tasks without skipping a beat.

The faster users realize a billing application is down, for example, the faster they can shift to email or other tasks. Across the organization, these downstream actions add up to an immense savings in time and attention that would otherwise be lost to miscommunication and confusion. This productivity advantage is the number one reason companies approach their NOC service as a business investment. **The value your NOC can return to the business is far greater than the investment necessary to make it effective.**

In addition to detecting issues, the NOC oversees corrective actions to restore functionality after an outage. Here, the NOC offers a golden opportunity to keep the business moving during downtime by improving communication between key stakeholders—both those whose work is impacted and those fixing the problem.

Unlocking this capability within your NOC requires a **centralized operational framework** to deliver information and take action at lightning speed—shortening response and resolution times while giving staff the information they need to adjust to the outage quickly.

To see more clearly how a NOC can save your business the high costs of low productivity, let's briefly revisit its basic functions.

What Does a NOC Do?

At its core, a successful NOC performs three functions:

1. Event Monitoring and Management

The NOC team responds to inputs from event monitoring and management systems as well as calls, emails, and other sources.

2. Ticketing

From the event monitoring sources, people and tools in the NOC create incident, change, and service request records.

3. Troubleshooting and Resolution

Processes and procedures guide the NOC to address each task.

A successful NOC logs every action taken and enables each impacted service to be restored as quickly as possible. While these functions may seem simple and straightforward, they require planning, implementation, and execution. In sum, **enabling your IT assets to meet and exceed demanding service levels requires a well-staffed, well-trained, and properly operationalized NOC equipped with the right processes and platforms.**

Enabling a Well-Functioning NOC

Establishing and running a well-functioning NOC takes diligence and coordination. At a high level, an organization needs to take these steps for its NOC to function optimally:

Understanding NOC Support Requirements

Setting the stage for NOC success goes beyond making a list of requirements. Those responsible for determining exactly what the NOC needs to do must have the knowledge and experience to ask the right questions from day one. At INOC, for example, an experienced and certified project manager works with each of our NOC clients to explore and clarify every support requirement in full detail. Having an experienced NOC expert leading this effort enables both parties to avoid the need for costly rework due to missed requirements.

Onboarding

Once the support requirements are identified in detail, those developing the NOC should employ a comprehensive onboarding checklist to ensure that each service component is fully operationalized. The onboarding team should collaborate with the NOC team to review the runbook, configuration items, knowledge articles, and documentation. The teams should work together to fine-tune the plan, train the NOC support staff, and confirm that all needs are met.

Ongoing NOC Service Monitoring

Once the NOC is up and running, it needs to be monitored and assessed from every angle. Tracking key NOC performance metrics is key. It's important to identify the targeted service levels, such as the uptime percentage, time to impact assessment, and mean time to repair. Once service levels are established and other important support metrics are identified and tracked, an overall picture of the NOC's performance can be obtained. The value of the operational framework will quickly become evident as advanced engineers spend less time putting out fires and more time on forward-thinking IT projects that support growth and expansion.

Continual Service Improvement

Continual service improvement means constantly reviewing every component of the NOC for gaps and opportunities. Armed with knowledge and intuition gained from firsthand experience, the continual service improvement team can anticipate challenges, spot opportunities, and recommend remedies and enhancements to improve the NOC.

Components of NOC Effectiveness

Five components are critical to the effectiveness of the NOC: (1) operational design, (2) establishing roles and responsibilities, (3) ensuring the right skills in the NOC, (4) building the NOC support infrastructure, and (5) overcoming the top challenges to NOC operations.

Let's look at each of these in detail.

1. Operational Design

Operational design is the key to unlocking a NOC's full capability and value. It provides a central framework with informed, documented guidance for each operational decision and action.

A look under the hood of any top-performing NOC will reveal such a framework. Most often, it's the factor that separates truly outstanding NOCs—those that have a measurable business impact—from those that only deliver basic support.

Developing an Operational Framework

The first consideration for developing a NOC operational framework is determining how the design will be created. Rather than putting a team together to hash out a framework from scratch, the resulting design will typically be far more robust and effective when an experienced NOC design team starts the development process with a proven framework that can be shaped to fit the requirements of your business and its IT infrastructure.

Whether you're taking on NOC operational design yourself or putting it in the hands of capable NOC experts, each component should take into account the three Ps: **people** (team with the right operational and technical skills appropriate for your environment), **process** (consistency through a standardized framework such as ITIL), and **platform** (a single consolidated view for the NOC team and other stakeholders.) Since these three Ps encompass everything that could be impacted by the NOC, this approach ensures nothing is left out of each operation you develop.

Incorporating Industry Standards

Different types of organizations require different outcomes from their NOC. Until recently, this meant incorporating different standards into the NOC framework depending on whether it was designed for an enterprise or service provider type of organization. For enterprises, the end users are usually internal staff. For service providers, the end users are typically customers. Each type of organization has traditionally required different guiding standards based on the outcome it needs to produce.

Today, however, the concept of IT service management based on the Information Technology Infrastructure Library (ITIL) service framework has gained momentum. ITIL provides significant guidance for developing, maintaining, and improving IT services, which makes it particularly useful for designing any type of NOC operation. ITIL has proven effective in a variety of applications and industries, thereby making the need for separate standards for enterprises and service providers largely obsolete.

As technology and software platforms continue to evolve, a well-conceived planning process that incorporates proven frameworks while abiding by long-standing best practices has become essential in designing a NOC operation that can adapt to change and keep up with innovation.

Designing Processes and Incorporating Tools

When you are developing specific elements of the NOC operation, your framework should offer well-defined process flows and incorporate tools to support each type of input into the NOC, such as phone calls, emails, and events. Phone and email tools should focus on helping the NOC achieve desired service levels for response time.

Today, with an operational framework that clearly identifies issues and offers processes to work through them quickly and easily, most issues that arrive through phone and email should be handled and initially routed or resolved by Tier 1 NOC engineers—freeing high-tier engineers to focus their attention elsewhere.

Here are a few things to keep in mind when designing processes and tools for handling NOC inputs:

PHONE CALLS — The framework needs the capability to identify specific details of a caller's IT service, such as the services they are signed up for, past service records, and other details that empower the NOC engineer to take action quickly.

EVENTS — Multiple alarm screens from different management platforms will hinder the NOC team's efficiency in diagnosing events. Bringing alarms into a single view, whether in a consolidated Network Management System (NMS) platform or a Manager of Managers, will be of immediate value.

EVENT CORRELATION — Event correlation—the process of analyzing relationships between multiple events to make sense of them—can be handled by a human alarm analyst, a rule-based system, machine learning, or a combination of these. Here, higher-tier engineers can play a short but meaningful role by performing advanced correlations that can then be passed to lower-tier engineers to handle with clear information in front of them. This approach frees higher-tier engineers to work on projects worth their time and expense. Once an event is ticketed, a quick and accurate diagnosis and action plan are needed so swift action can be taken.

Key Considerations: NOC OPERATIONAL DESIGN

- Is your NOC fully aligned with the ITIL framework?
- Does your team possess the skills needed to design and implement a framework-based NOC operation?
- How well does your current NOC serve your particular end users?
- Does your NOC's operational framework clearly address each of the three Ps: people, process, and platform?
- Does your NOC employ the right tools and processes to handle phone calls, emails, and events?

2. Establishing Roles and Responsibilities

The NOC team's key responsibilities encompass a series of tasks presented in the ITIL framework:

- Event Monitoring and Management
- Incident Management
- Problem Management
- Capacity Management
- Change Management

While the ITIL framework includes other processes, in our experience these five are the most important to address. Let's briefly look at them through a practical lens.

Event Monitoring and Management

Event Monitoring and Management allows the NOC to monitor, detect, and process events and faults related to the organization's infrastructure and systems. Events can consist of alarms from systems, calls from internal staff (or customers), and email or chat.

The NOC team uses a single or as is common, multiple tools, including Network Management Systems (NMSs), Element Management System (EMSs), Application Performance Management (APM) tools, and others. These platforms receive and filter messages from devices, servers, cloud instances, applications, and other infrastructure using protocols such as SNMP, TL1, WMI, and, more recently, gRPC and gNMI, among others. Once an event is detected, it's evaluated, correlated, and acknowledged, and if further management is needed, it's logged into an incident or ticket.

Incident Management

Incident Management is the core process of any NOC. Using the NOC's IT service management platform or ticketing system, this process provides support when a network, system, or application event requires action. The event is recorded in a ticket with information in different fields. Tickets are handled by NOC engineers

and also sent to other personnel as needed in the form of an email, a call, or a message requesting action to address an issue. These communications also include periodic updates and notifications until the incident has been closed. Incident tickets collectively act as a record of all work efforts in the NOC and allow for reporting that can help manage NOC workflow and resources.

Problem Management

Problem Management includes all the activities needed to diagnose the root cause of incidents and request changes to resolve those problems. Problem Management differs from Incident Management as the focus is to investigate and identify the root cause of an incident rather than its effect. Typically, Problem Management requires greater engineering skills to review the trends leading up to an incident, scour logs for indications that point to possible causes of the failure, and formulate plans to prevent future incidents. The Problem Management service also maintains information about problems and workarounds for use by Incident Management personnel.

Capacity Management

Capacity Management oversees the performance, utilization, and capacity of infrastructure components to ensure that the client's service level targets are achieved. Capacity Management should ensure that business capacity, service capacity, and component capacity needs all continue to be met. Senior engineers' regular reviews of reports and alarm thresholds, taking into account the desired business outcomes and the impact of utilization on business operations, will ensure that evolving capacity needs are addressed in a timely manner.

Change Management

The goal of Change Management is to reduce risk when changes are made to the supported infrastructure environment. This function includes identifying the types of changes the organization anticipates and establishing how each change should be handled to reduce the impact on the organization. Processes and controls are generally oriented around three types of change:

- **Standard changes** are routine and low-impact, like resetting passwords.
- **Emergency changes** must be addressed promptly, such as by rerouting network traffic when the primary WAN uplink at a regional office is unstable.
- **Normal changes** are planned in advance and might include upgrading the operating system on a server cluster, for example. This type of change would be managed through a review process to ensure proper planning.

A **Change Advisory Board** should review and set policies for all these changes. The Change Advisory Board helps mitigate risk by ensuring all possible impacts of the change have been taken into consideration and a proper plan with a recovery process is in place.

Key Considerations: ROLES AND RESPONSIBILITIES OF A NOC

- Does your NOC adequately address each of these five key processes?
- Does the NOC's reporting capability deliver meaningful metrics in each of these areas?
- Are you using recorded incident records to help manage NOC resources appropriately?
- Are NOC engineers reviewing trend data, conducting effective root cause analysis, and taking preventive action?
- Does the NOC review and adjust your IT infrastructure capacity in anticipation of the organization's changing business needs?
- Does your NOC have a Change Advisory Board to manage the risks posed by changes?

3. Ensuring the Right Skills in the NOC

NOC engineers need a variety of skills to keep your network, infrastructure, and applications up and running. Diverse technical knowledge, including knowledge of various network technologies, cloud environments, server operating systems, virtualization, storage systems and applications, is required to run the modern NOC. This demand for skilled human resources in a 24x7 environment can pose a considerable and often insurmountable challenge for many organizations.

In addition to these well-established skills needed in the modern NOC, innovations demand new types of skills. Machine learning and artificial intelligence in particular pose new challenges that don't always lend themselves to time-tested best practices. Even many seasoned NOC engineers, for example, haven't dealt with networks becoming more "aware" of the traffic that runs through them. Developing skills that complement machine intelligence is just one example of the evolving challenges that those who work in the NOC will need to overcome.

Prioritizing NOC design (along with the right training programs and tools) to maximize your team's capabilities from the start saves an incredible amount of expensive, labor-intensive work as the NOC comes to life. Understanding the required skill set early on can help you identify the correct staff to hire and drives the selection of tools to manage the infrastructure over time. In addition, a rigorous, ongoing knowledge management and training program is important to ensure the entire NOC team is up to date on all changes made to the supported infrastructure.

Key Considerations: ENSURING THE RIGHT SKILLS IN THE NOC

- Do you currently have the internal resources to design, implement, and manage a NOC effectively?
- Are you aware of any skill gaps across your NOC team?
- Would significant changes or updates to your NOC support operation create a need for additional skill sets?

4. Building the NOC Support Infrastructure

The Structured NOC

Even the most skilled engineers and system administrators will struggle without the proper NOC support infrastructure. All too often, however, businesses prioritize hiring and overlook the structural elements that empower people to do great work. A well-structured NOC with the right tools to support each function can boost efficiency and reduce costs dramatically.

In fact, the structure of the NOC—the way its components are organized and connected to one another—may be the single most powerful factor that determines the NOC's overall success.

A structured NOC, as we've come to call it, demonstrates its value most clearly when it's implemented in a NOC environment where little to no intentional structure existed before. In just weeks or months, teams will see response times steadily drop and support activities migrate to appropriate tiers—lightening the load on advanced engineers while enabling the NOC to resolve issues faster and more effectively across the board. When a structured NOC is implemented, we generally see 60% to 80% of all NOC issues addressed by Tier 1 staff, rather than involving advanced engineers in nearly all issues.

Supporting the NOC

While the NOC delivers support, it also requires support to perform at its best.

Successful NOC operations, particularly in larger organizations with complex infrastructure, require a combined effort of the NOC team and critical support teams.

The INOC team, for example, utilizes the following roles and functions encompassing the initial service transition, close-knit customer experience management, and everything in between.

SERVICE TRANSITION TEAM

This support function sets outsourced NOC providers apart from in-house teams, which often have limited resources. To set the NOC team up for success, a dedicated service transition team draws on years of onboarding experience to ensure nothing is overlooked when the NOC begins to operate. After the initial service transition (onboarding) phase, this team ensures that any changes needed to address ongoing shifts in the infrastructure are made effectively.

PLATFORM INTEGRATION AND DEVELOPMENT TEAM

This team supports NOC integrations with a range of client, third-party, SaaS, cloud, and OEM-specific systems, including trouble ticket systems, NMSs, EMSs, device types, operating systems, cloud providers, and application infrastructure. Clients also get custom monitoring functionality to ensure that the NOC has a comprehensive view into their entire infrastructure.

REPORTING TEAM

Meaningful operational metrics play an underappreciated role in keeping staff morale high. That's why the NOC deserves a team devoted to setting and evaluating daily, weekly, and monthly performance objectives. Reporting experts identify the metrics that are most meaningful and applicable, reflecting the size and scale of the operation and the organization's key performance indicators. Metrics like first-call resolution, time to action, mean time to repair, and number of tickets and calls handled provide operational visibility and can represent points of pride for accomplishments within the NOC.

QUALITY CONTROL AND ASSURANCE

A well-managed quality control or service assurance program enables the NOC to identify and resolve problems before they significantly impact your organization or customers. At INOC, for example, our internal quality control program looks at a range of metrics to understand how our service is performing for each of our clients. NOC managers follow up on all client feedback with an internal review of the service to evaluate responsiveness, adherence to runbook procedures, customer interaction, and technical troubleshooting to name a few. Such quantitative and qualitative measures, and the resulting feedback, reduce the likelihood of recurring problems. Monthly and quarterly stakeholder service reviews ensure that customer expectations continue to be met.

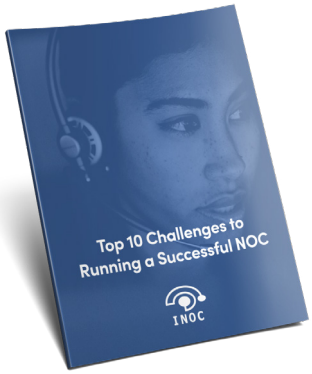
If adding an extra layer of support sounds expensive, keep in mind that a tiered NOC structure, typically routes between 60% and 80% of all NOC issues to Tier 1 NOC engineers, enabling higher-level engineers to devote their time and attention to other projects. With the right support structure in place, Tier 1 engineers can get expensive high-tier support only when they need it, reducing costs across the board.

Key Considerations: BUILDING THE NOC SUPPORT INFRASTRUCTURE

- Does your NOC have a clearly defined structure to guide its operations?
- Does your NOC have adequate support?
  - If you're planning a NOC, do you have the resources to support the transition adequately when the NOC begins to operate?
  - Is your NOC able to support integration with in-house and third-party systems?
- Does your NOC report meaningful metrics that reflect your business's operational goals?
- Are you conducting regular reviews to ensure that you're meeting customer expectations?

5. Overcoming the Top Challenges to NOC Operations

When a NOC consistently fails to meet established service levels, the root cause—and the necessary fix—is typically an operational deficiency. Understanding these operation challenges will help you overcome them:



Check out our white paper **Top 10 Challenges to Running a Successful NOC** for a deeper dive into these challenges.

GET THE WHITE PAPER →

- Lack of tiered organization/workflow
- Lack of meaningful operational metrics
- Difficulty in staff hiring, training, and retention
- No standardized process framework
- Lack of a business continuity plan
- No quality control or assurance
- Disparate tools and platforms—no comprehensive view
- Lack of documentation and runbooks
- Lack of scalability
- High operational costs

Think of this list as the tips of multiple icebergs. Lurking beneath the surface, a number of complex, interconnected problems can be incredibly difficult to fully understand and resolve.

All too often, organizations with a poorly designed NOC find themselves dealing with these operational challenges. Just as often, the same lack of operational capability ironically prevents a comprehensive solution. Without the visibility enabled by well-documented processes, for example, organizations often resort

to hiring expensive engineers just to keep the infrastructure and applications up and running. Throwing people at the problem just costs your organization money—it doesn't solve the underlying issue.

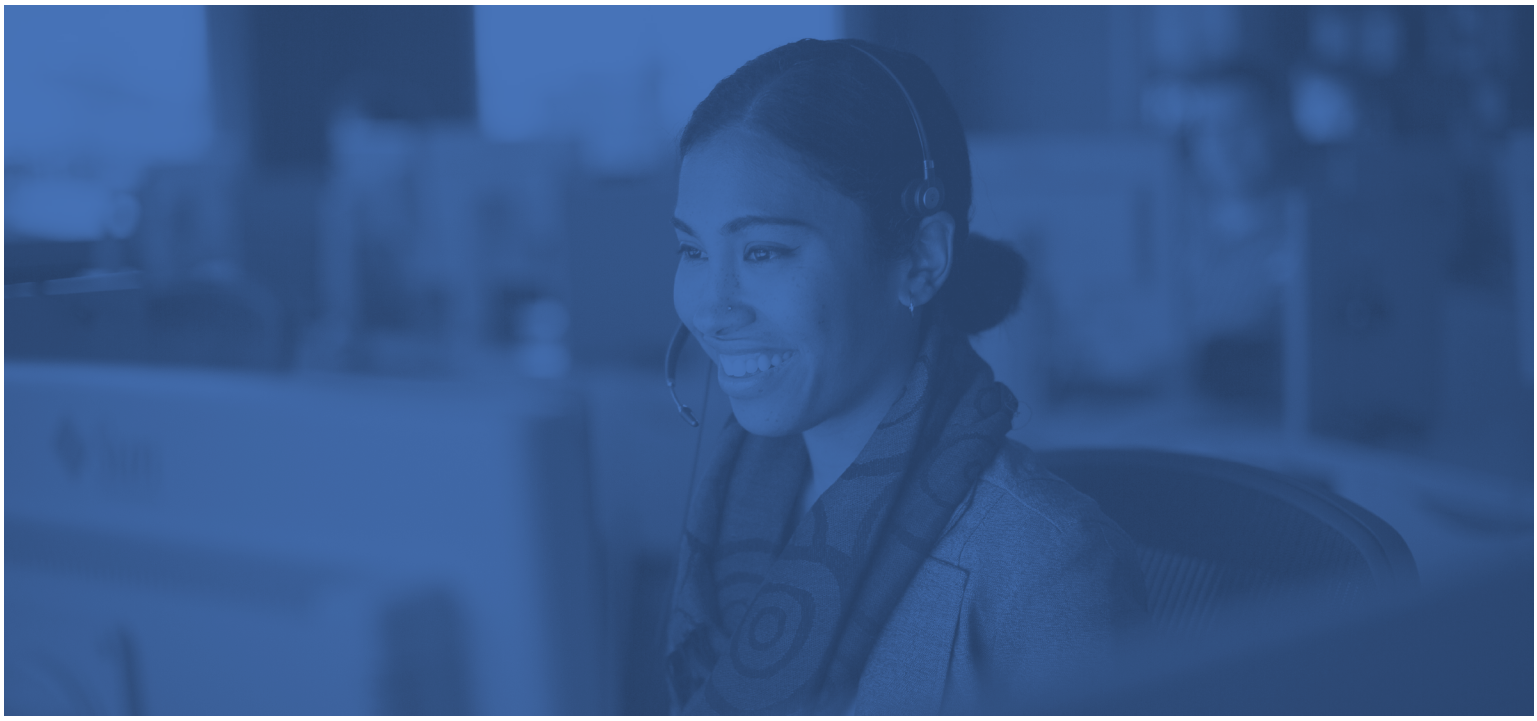
Instead, anticipating the top challenges and addressing them proactively goes a long way toward meeting the constantly growing demands on your organization's IT resources.

Whether you are building or managing a NOC, keep in mind that simplifying your tools, building your documentation, establishing process flows, and ensuring the NOC can adapt to changing business needs are far better investments. These steps aren't just nice to have—they serve as genuine investments in business productivity, with ROI you can measure in time and money.

Even the simplest examples clearly illustrate the value of a well-designed NOC. By investing in automated tools that analyze alarms to identify affected services, for example, you can reduce troubleshooting time substantially from 10 or more minutes per event to just a few minutes of human validation, leading to greater uptime. You can easily calculate the ROI to your organization in terms of increased productivity. A website down for an hour could cost thousands of dollars in lost revenue. 90 minutes of circuit downtime could decrease productivity by 50%, lowering staff efficiency and morale.

Key Considerations: OVERCOMING THE TOP CHALLENGES TO NOC OPERATIONS

- Does the list of challenges sound familiar to you?
- If you're planning to implement a NOC, have you designed your operational framework to anticipate and prevent these challenges?
- Have efforts to analyze the root causes of issues been hindered by a lack of effective tools or processes?
- Have you been tempted to hire more NOC engineers, hoping they can solve all the problems with your IT infrastructure?



Final Thoughts and Next Steps

NOC teams tend to be the unsung heroes. But when this vital function goes underserved, its value to the organization immediately becomes clear.

Investing in your NOC maximizes its power as a business driver. A well-designed NOC operation, staffed with the right people and tools, will maximize uptime of your infrastructure and applications by reducing incident response time, identifying problems, ensuring network and infrastructure capacity, and reducing the impact of changes.

While it's easy to talk about the importance of a structured NOC, it's another thing entirely to bring that idea to life in your organization. Success requires careful planning and care. When the worst happens, is your organization prepared to respond? Even a well-equipped organization can almost always find new efficiencies and gain a competitive advantage by enhancing its IT support environment.

Use the worksheet below to help identify the opportunities INOC can help you tackle through our award-winning NOC operations consulting or 24×7 outsourced NOC support. Then, **contact us** to get the conversation started.

WORKSHEET

Preparing for NOC Success

- How would you rate your NOC's overall service design and operation?
- Have you implemented a service catalog detailing the services your NOC performs?
- Do you use service level management to set your service level agreements and service level objectives? Do you report performance on a regular basis?
- Do you track changes to your infrastructure and have a change review process?
- When onboarding new components into your NOC, do you follow a process to review those changes and ensure they are consistent and accurate?
- What percentage of issues does your Tier 1 response team currently handle?
- Do you continually review incidents for opportunities to improve operations and tools?
- Does your NOC have the appropriate support personnel to assist with process flow, technology, and improvements in responsiveness?

Unlock the full potential of your IT infrastructure and keep it running 24x7.

Have questions?

Want to learn more about building, optimizing, or outsourcing your NOC?

Our NOC solutions enable you to meet demanding infrastructure support requirements and gain full control of your technology, support, and operations. **Contact us today and get the conversation started.**

info@inoc.com

+1-877-NOC-24X7

If you prefer, head to our contact page to tell us a little about yourself, your infrastructure, and your organization's challenges. We'll follow up by phone or email within one business day.

CONTACT US →

ABOUT INOC

INOC is an ISO 27001:2013 certified 24×7 NOC and an award-winning global provider of NOC Lifecycle Solutions®, including NOC support, optimization, design, and build services for enterprises, communications service providers, and OEMs. INOC solutions significantly improve the support provided to partners' and clients' customers and end users.

INOC assesses internal NOC operations to improve efficiency and shorten response times, and provides best practices consulting to optimize, design, and build NOC operations, frameworks, and procedures. Proactive 24×7 NOC support is provided with several options, including North America, EU, or APAC only or global integrated NOCs. INOC's 24×7 staff provides a hands-on approach to incident resolution for technology infrastructure support.