SERVICE. NOT SOFTWARE.®

WHITE PAPER

Top 10 Challenges to Running a Successful NOC — and How to Overcome Them

A majority of network operations centers fail to meet the service levels demanded of them. Make sure yours isn't one of them.

PRASAD RAO

INTRODUCTION

The network operations center (NOC) provides the foundation for an effective and scalable technical support operation, which is critical in today's "always-on" environment. Yet, a majority of NOCs, in both the service provider and enterprise markets, fail to deliver the desired service levels while consuming a significant amount of management and financial resources.

The biggest reason for this failure is that companies do not have an authoritative blueprint to follow. A blueprint outlining the aspects of a successful NOC will be different for each organization, as it depends on company strategy, technology infrastructure, tools and service requirements. However, there are a number of common challenges in running an efficient and effective NOC. Here are the 10 we see most often:

1. Lack of tiered organization/workflow
2. Lack of meaningful operational metrics
3. Difficulty in staff hiring, training and retention
4. No standardized process framework
5. Lack of a business continuity plan
6. No quality control or assurance
7. Disparate tools and platforms — i.e., no "single pane of glass"
8. Lack of documentation and runbooks
9. Lack of scalability
10. High operational costs

This paper provides insight into each of these challenges and how they can be addressed.

Prasad Rao is Co-Founder/President and Chief Operating Officer of INOC. An organizational efficiency and quality control expert, Prasad has 25 years of experience in operations, finance and business development in the IT and manufacturing industries. Prior to INOC, he was Director of Engineering at RC Machine, where he oversaw the engineering of automotive production machines. He was also co-founder and chief executive of Vidhata Plastics, a pioneering manufacturer of polyurethane shoe soles. A graduate of the Indian Institute of Technology-Madras, Prasad holds an M.S. in industrial engineering from the University of Illinois.

1 TIERED ORGANIZATION AND WORKFLOW

Failing to organize NOC activities and the subsequent workflow based on technology and skill level is one of the biggest hurdles in building a successful NOC.

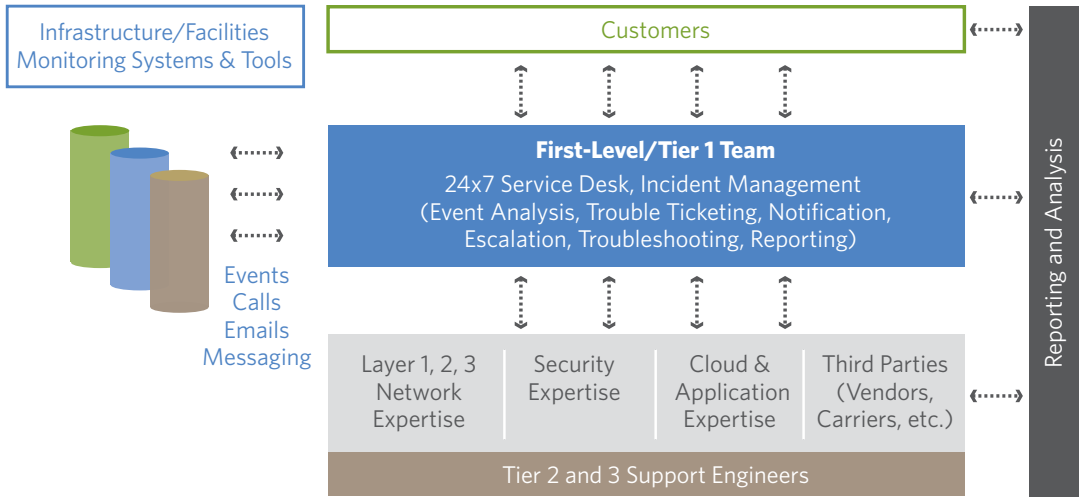
NOC activity can be classified into the following broad categories:

- Monitoring events from technology infrastructure and facilities — e.g., Layer 1, 2 and 3 networks, circuits and servers (physical, virtual and cloud), applications, databases, and power and building systems
- Managing support requests from customers and technical staff in the form of phone calls, emails and tickets
- Managing incidents resulting from events and support requests
- Managing configurations and changes, provisioning equipment, services and circuits, and maintaining documentation
- Reviewing periodic service reports

Most of these are 24x7 activities that require dedicated resources. A tiered operational support structure enables managers to leverage the lower-cost first-level or Tier 1 team to perform routine activities and free up higher-level or Tier 2 and 3 technical teams to focus on more advanced support issues.

Figure 1 shows a well-organized tiered NOC support structure, central to which is the Tier 1 team that uses monitoring tools and interacts with end-user help desks, Tier 2 and 3 engineers, and third parties. Information flows between the various entities within a well-defined process framework.

FIGURE 1: **TIERED NOC SUPPORT STRUCTURE**



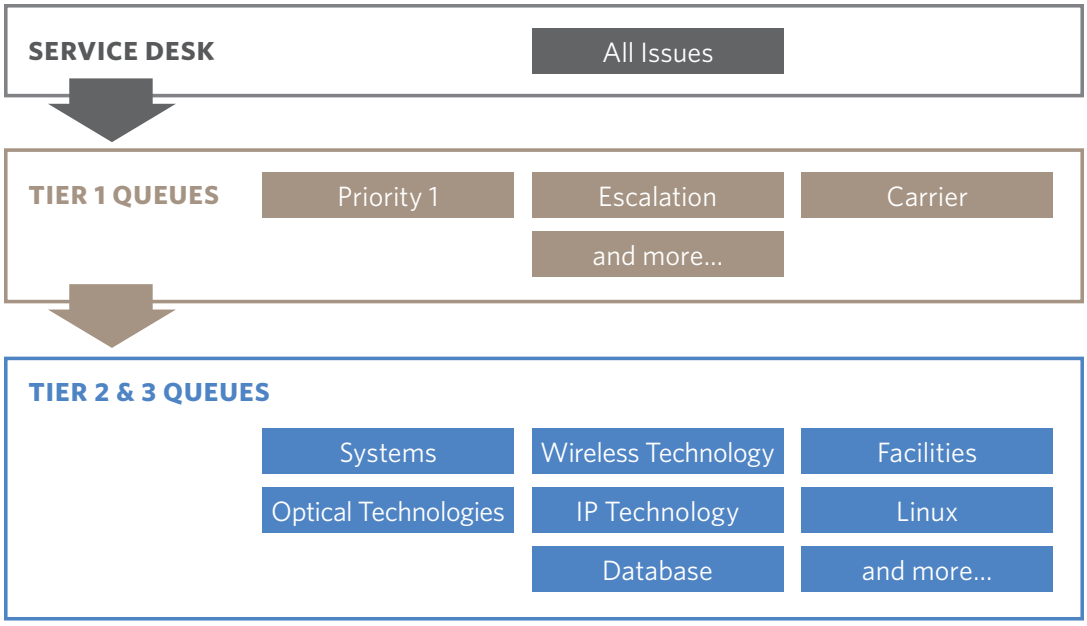
Employing this structure, a NOC can effectively resolve 65 to 75% of incidents at the Tier 1 level, and advanced issues can be escalated to specialized IT staff. This enables the support group to handle the events, service requests and incidents at the appropriate tier, more quickly achieving resolution.

Without properly managing workflow, a NOC can be easily overwhelmed by the "wall of red." Issues should be prioritized and organized into a set of queues, each of which can be handled by the appropriate group. The following variables play an important role in determining workflow:

- Service-level agreements (SLAs)
- Technology
- Technician skill level

Figure 2 shows how a set of issues can be broken up into queues and assigned to groups based on skill set.

FIGURE 2: **SAMPLE WORKFLOW QUEUES**



2 MEANINGFUL OPERATIONAL METRICS

Meaningful operational metrics are vital not only in running a successful NOC, but also in keeping staff morale high.

Anyone who works in a NOC likely hears statements like these on a routine basis: "We are always busy," "I feel like we can never catch up," and "My coworkers are not pulling their weight." These sentiments are understandable, given the fast-paced environment of a NOC and constant multitasking that is required.

Thus, it is imperative that performance objectives be set and evaluated on a daily, weekly and monthly basis. The amount of data available to a NOC is daunting; the key is to choose the metrics that are most meaningful and applicable to your specific operation. These include metrics reflecting the size and scale of an operation and key performance indicators (KPIs) that reflect the performance of an operation as compared to a set of organization objectives.

KPIs to consider include first-call resolution, percentage of abandoned calls, mean time to restore, and number of tickets and calls handled. Such metrics provide visibility into the operations, giving the NOC an objective and the team a sense of accomplishment. Table 1 shows a sample set of operational metrics.

TABLE 1: SAMPLE OPERATIONAL METRICS (SERVICE PROVIDER)

	Week 25	Week 26	Week 27	Week 28	Week 29
Alarms	3,284	4,349	9,982	15,126	6,956
Calls	162	159	206	232	213
Average Duration	0:05:39	0:05:19	0:04:19	0:05:16	0:04:49
Tickets	231	309	312	337	342
KPIs					
Response Time (minutes)	9	12	13	14	11
Call Hold Time (seconds)	33	32	36	28	21
Complaints	2	5	0	0	0
Mean Time to Restore (hours)	3.5	3.7	2.9	3.7	3.3

3 STAFF HIRING, TRAINING AND RETENTION

Running a 24x7 NOC requires staffing three shifts a day, 365 days a year. The following factors should be considered in determining a staffing strategy:

NOC Organization Structure. Effectively staffing a 24x7 NOC starts with a well-organized structure. The tiered NOC support structure and workflow queues discussed in Section 1 are a good starting point for determining the skill level required of your NOC staff.

Figure 3 shows an example of a skills-based NOC structure that can be adapted not only to support your 24x7 NOC requirements, but also to provide a growth plan for employees that is essential for retention. Once the NOC is organized and the position descriptions are created, your HR team should be armed with clear directives for hiring and retention.

FIGURE 3: SAMPLE HIGH-LEVEL NOC STRUCTURE

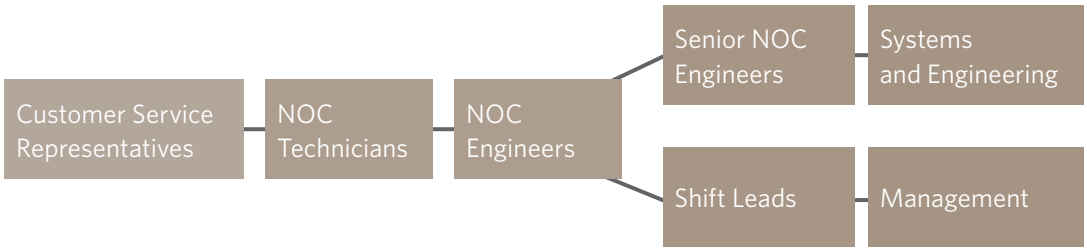


TABLE 2: SAMPLE NOC UTILIZATION METRICS

Total for September 2014	
Alarms	95,307
Tickets Created	6,090
Ticket Time (hours)	3,365
Calls Inbound	4,852
Average Duration Time (seconds)	187
Calls Abandoned (>60 seconds)	39

	Shift (hours)			
Day of Week	1st	2nd	3rd	Total
Sunday	142	90	44	276
Monday	270	152	57	479
Tuesday	325	126	86	537
Wednesday	362	133	141	636
Thursday	352	109	116	577
Friday	394	123	68	585
Saturday	148	75	52	275
	1,993	808	564	3,365

Utilization Metrics. Consider the overall activity of your NOC, including the volume of calls, emails and alarms handled by hour of day, day of week and type of support engineer, as well as the duration of incidents. Table 2 shows an example of such metrics for a specific NOC. Data like this can be translated into a working schedule for each type of support engineer needed to satisfy the staffing requirements of your NOC.

Benefits Plan. Be sure to take into consideration the benefits that your company provides for employees. For example, if your company provides 10 holidays and four weeks of PTO per employee, these hours need to be accounted for to ensure that your NOC runs smoothly.

Training. A NOC training program should include initial on-boarding as well as ongoing training. It may take up to six months of various classes and on-the-job training before an engineer is ready to take on NOC support responsibilities. After work has begun, monthly or quarterly training sessions should be scheduled to keep engineers' skills fresh and to update the support team on new types of services, new customer requirements and new equipment.

Retention. A certain rate of attrition within the NOC should be taken into account, based on your historical data and on industry standards. Factors that affect retention rates include company culture as well as NOC organization — i.e., whether there's a clear path for employee growth from one level to the next or to other departments within the organization.

By making these calculations, you can better plan for staffing and training needs. For example, assuming that a typical engineer works five years in your NOC (a retention rate of 80%), you'd need to hire an additional 20% of staff each year.

4 STANDARDIZED PROCESS FRAMEWORK

A lack of consistency is one of the main reasons NOCs don't perform at optimal levels. The best way to create consistency is through a standardized process framework. Such a framework provides a NOC with a set of specific procedures for handling various support situations. There are several process and management frameworks to choose from, including MOF, FCAPS and ITIL.

ITIL (IT infrastructure library) is a widely used framework that is useful in achieving the ISO 20000 certification. It provides best practices to follow when delivering technology support services as well as the flexibility to include your organization's custom procedures under its umbrella of life cycle stages.

Process frameworks can be overwhelming when considered in their entirety. We recommend first tackling the specific areas that are the biggest challenge for your organization. Typically, these are incident management, problem management and service desk. Once these functions are standardized, you can move on to other priority areas such as change management and service continuity management.

It is critical to get your whole organization involved in the implementation of the process framework as well as in ongoing education.

It is critical to get your whole organization involved in the implementation of the process framework as well as in ongoing education. Training is essential to get all staff talking the same language and following the same guidelines. Comprehensive information and training are available for ITIL, ISO 20000, FCAPS and other methodologies.

5 BUSINESS CONTINUITY PLAN

A business continuity plan (BCP) is essential for managing risk in your NOC operations. It provides a blueprint for NOC staff and management to follow in recovering from a disaster or other adverse situation. When properly executed, it ensures that operations recover quickly and effectively.

The lack of an effective BCP could result in the following problems:

- Loss of business
- Damage to reputation/brand

- Loss of customers
- Loss of staff
- Loss of or damage to property and premises
- Negative impact on insurance

Key representatives from a cross-section of the organization need to be involved in creating a BCP. Keep in mind that this may include outside vendors.

The first step in developing a BCP is to determine all threats that could interrupt regular operations. These include severe weather, facility access restriction or infrastructure failure, critical asset impairment, security incident, key personnel loss, a crime and others.

The next step is determining the most significant tasks required to continue operations. For example, consider the minimum number of essential people required, and which assets, tools and information are critical.

The plan must include relocating existing operations to a backup location if a disaster occurs at the primary NOC facility. For example, if a mandatory evacuation occurs at the working NOC location, then people must relocate to the secondary site to continue operations as expediently as possible.

The plan should also outline procedures for recovering quickly from different levels of disaster — from short-duration problems, such as loss of utilities and equipment failures, to longer-duration problems, such as a regional disaster barring access to the facility for several days/weeks or a permanent loss of the facility.

In summary, a business continuity plan should include the following:

- An analysis of all organizational threats
- A list of action items required to maintain operations, both for short-term and long-term interruptions
- Easily accessible contact information for key stakeholders
- An explanation of where/how personnel should relocate if there is an interruption in operations
- The steps required to make the backup site(s) operational
- How all the areas within the organization need to collaborate in executing the plan

The BCP must be readily accessible to the management team at all times and should be rehearsed at least quarterly and regularly audited for possible improvements.

The BCP must be readily accessible to the management team at all times and should be rehearsed at least quarterly and regularly audited for possible improvements. The testing should also include failover of all critical assets to ensure that failure of a single asset or multiple assets cannot cause a prolonged outage.

6 QUALITY CONTROL AND ASSURANCE

A NOC team must measure service quality and provide quality assurance on a continuous basis or it risks losing customer satisfaction and compromising its reputation. And effectively and consistently executing a runbook — i.e., processes and procedures — is paramount to meeting a NOC's service level requirements.

Core to meeting these objectives is the detailed monitoring of key network and IT assets and services. This monitoring, data collection and correlation — typically accomplished using a variety of protocols and tools — is the entry point into incident handling and problem management processes. Additional sources of data include calls, emails and other inputs. The NOC runbook, created during the on-boarding process and updated regularly, is key to what follows next. Documenting agreed-upon processes and procedures for the specific customer environment provides the NOC team with an essential operational reference.

A good quality or service assurance program allows the NOC to identify and resolve problems before they impact customers or the business in a significant way.

A good quality control program monitors and measures primary aspects of the NOC service — the key performance indicators referenced in Section 2. These KPIs provide much-needed visibility into NOC support activity, responsiveness and effectiveness. NOC management can use this information to ensure, for instance, that stated objectives for event-to-action times and first-level incident resolution are being met for each customer. Quality control also detects chronic issues so management can find appropriate solutions — for example, correcting relevant runbook procedures, ensuring complete documentation is available to the NOC or providing additional staff training. A monthly audit of a subset — say, 5% — of all tickets created is an important part of ongoing review. Staff mentoring is also key to quality control and helps ensure high levels of customer satisfaction.

A good quality or service assurance program allows the NOC to identify and resolve problems before they impact customers or the business in a significant way. A quality assurance review begins when a customer reports dissatisfaction with any aspect of the NOC service. NOC management follows up with an internal review of the service —

responsiveness metrics, adherence to runbook procedures, customer interaction and technical troubleshooting, to name a few. Such quantitative and qualitative measures and the resulting feedback lower the probability of the same problem reoccurring. Monthly and quarterly reviews of the service with stakeholders ensure that customer expectations continue to be met.

7 PLATFORM INTEGRATION

An efficient NOC has the ability to receive and process alarm or event information from multiple sources and present it in a single, consolidated view for staff to act on. This consolidated view is commonly referred to as a "single pane of glass." In addition, there is a need to bring voice, email, text, customer portals, knowledge bases, documentation and workflow management tools into the NOC, each potentially with its own platform.

Without integration of these tools and platforms, NOC personnel are faced with tracking and managing multiple screens for event information; manually collecting information from multiple sources for the purposes of documentation, notification and escalation; and then attempting to manage workflow toward service restoration. This makes it nearly impossible to monitor and report on SLA metrics, let alone optimize performance. The results inevitably include operational inefficiencies, missed SLAs and undue stress on staff.

Figure 4 depicts the various tools that are required for a NOC to function and that should be integrated into a single NOC platform. Following is a brief description of each:

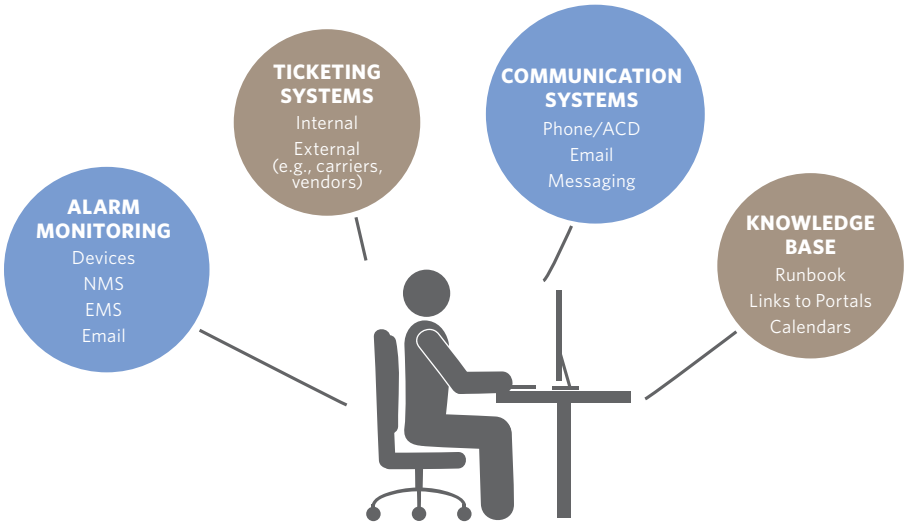
Alarm Monitoring. Platform integration needs to consolidate alarm or event data from various sources. These can include:

- Direct devices and services monitoring
- Vendor element management systems
- Network management systems
- Custom application management tools
- Fiber and facilities/building management systems
- Environmental monitoring (heat, power, intrusion, water, etc.)

Ticketing Systems. Ticketing systems are used for documentation and workflow management and need to be tied into the single NOC platform. In addition, customers may use their own ticketing systems, which also need to be integrated into the NOC platform for documentation and efficient workflow between parties.

Communication Systems. For efficient communications, phone, email and messaging systems need to be linked into the NOC platform.

FIGURE 4: NOC TOOLS



Knowledge Base. The NOC runbook containing work instructions for successfully managing an event to completion is a fundamental requirement for good NOC support. A detailed runbook also provides access to contact lists and calendars for notification, escalation and dispatch, network, site and building diagrams, troubleshooting procedures, equipment manuals, customer and third-party databases, and more. Integrating knowledge-base access into the NOC platform allows the support team to quickly navigate and find the relevant information needed to resolve an issue.

Effective integration requires a good understanding of process and workflow management, the ability to map out the processes with relationships identified, and the ability to create appropriate linkages between the tools and platforms.

Done right, an integrated platform provides a single, consolidated view for NOC personnel. The result is an efficient workflow, effective troubleshooting and fewer errors — all of which mean greater quality control and performance optimization.

8 DOCUMENTATION

Failure to build runbooks, document workflow processes, create structured databases for storage and retrieval of information, and record business results for later analysis and optimization will severely impede the ability of a NOC to function well over the long term. Too often, services are added and changes are made without proper documentation. This limits the ability of the NOC to resolve an issue when it arises.

Poor documentation often stems from a lack of resources and the expertise required to map out processes and create work instructions and documents. Instead, key people simply "know what to do" and new staff learn by "seeing and doing" alongside an experienced mentor.

In addition, performance metrics that can be obtained from network and monitoring systems, ticketing systems and back office tools are often overlooked. These metrics are critical for analyzing performance, predicting failure and laying the groundwork for ongoing quality control and process improvement. Without an understanding of alarm activity, ticket activity, and common causes for outages and trends, management is limited to responses that are reactive and tactical, rather than proactive and strategic.

Beginning with the service catalog, it is necessary to document the tools and procedures needed to deliver NOC services successfully. Technical writers can often be invaluable in this process.

9 SCALABILITY

Scalability is the ability of a NOC to handle a growing amount of work without compromising the level of service. Typically, business plans include initial funding, sales and marketing, system build-out, operations support and the business guidance needed to meet the projected growth. What business plans sometimes don't take into consideration are predictable growth and process planning.

Often, for example, sales for a young company take off, with key managers focused on new clients and getting technical services delivered to meet service launch dates. The same technical and operations resources are then tasked with the ongoing support of these services, severely impeding the organization's ability to manage its growth. The result is predictable: customer dissatisfaction.

The same technical and operations resources are then tasked with the ongoing support of these services, severely impeding the organization's ability to manage its growth. The result is predictable: customer dissatisfaction.

The ability to grow or absorb expansion requires careful consideration of the following factors:

Staffing. It is essential to measure the staff utilization percentage derived from various NOC activities (described in Section 2). Keeping this below 80% allows the NOC to absorb growth while allowing enough lead time for recruiting additional resources.

Systems and Network. A distributed redundant architecture allows for systems to grow and expand. The ability to easily deploy additional server resources on demand is important in order to handle sudden spikes in growth. The performance of the systems and network (bandwidth, CPU, memory, etc.) needs to be monitored closely to make sure there is enough capacity to handle growth.

Tools. Tools used by the NOC (e.g., monitoring tools, ticketing systems, knowledge base) to deliver the service must have additional capacity built into them for the projected growth. It is not uncommon for tool performance to reduce dramatically if tools are not designed for growth that results in service-level degradation and loss in productivity.

Process Standardization and Training. A consistent process framework and methodology for delivering high-quality service is one of the key features of a scalable NOC. Management should choose and adopt a process standard that fits their product and industry needs. NOC staff can then be trained to follow the established company standards.

10 OPERATIONAL COSTS

There are several components that make up the cost of running a 24x7 NOC. The major ones are described below.

Staff. The staff required to support a 24x7 NOC include not only front-line technicians and engineers, but also back-end support groups such as systems and network engineering, service transition, human resources and customer advocacy.

Training. Resources need to be allocated for training NOC staff when they are initially hired, when on-boarding new customers, and whenever changes are made to existing support or new technologies are introduced.

Quality Assurance. An objective quality assurance program is needed to address customer concerns and maintain service-level agreements.

Systems, Networking and Security. Systems, network connectivity and security controls need to be deployed in either a data center or the cloud to house the various tools and applications required by the NOC to operate. Resources for ongoing support need to be included.

Software Licensing. A NOC requires various tools for monitoring, troubleshooting and resolving issues. These include network and element management systems (NMS/EMS), trouble ticketing systems, knowledge bases, portals and configuration management databases (CMDB).

Infrastructure and Facilities. A NOC must be designed and maintained to enable smooth workflow and communication among staff. Redundancy and business continuity are essential to mitigate risk.

Compliance. NOC services must comply with various regulatory and industry standard requirements.

All of these components present a formidable operating expense but have to be considered in building a successful NOC. Too often, NOCs are built considering only a subset of the above components, and as a result, they struggle to scale and deliver on the required service and financial objectives of the organization.

CONCLUSION

Addressing the 10 most common challenges faced by NOCs will allow your organization to build a successful blueprint for your own operations that will meet the ever-increasing service levels demanded by customers in this age of "always available" expectations. The return on investment is realized through lower operating costs, less downtime, and greater employee and customer satisfaction.

Prasad Rao thanks everyone at INOC for their contributions to this white paper.

INOC is a global provider of 24x7 Network Operations Center (NOC) monitoring and reporting solutions. Our NOC delivers timely and critical network information to clients to improve the uptime, security and availability of network and IT infrastructure. INOC's NOC monitors and reports on national, regional and metro networks, as well as servers and applications for carriers and enterprises throughout North America and Europe.

For more information on INOC and its services, send an e-mail to info@inoc.com or call 1-877-NOC-24X7 (1-877-662-2497). You will also find additional information at our website, www.inoc.com.