10 Exchange Place, 17th Floor
Jersey City, NJ 07302
Email: sales@itbd.net

10 Questions to Ask Your Prospective NOC Service Provider

There are plenty of good reasons for MSPs to outsource their NOC to a service provider, but doing so comes with inherent risk—especially if you don't do your homework first. Today's MSPs are entrusted with client's financial data and other sensitive information, so it's never been more important to carefully evaluate potential service providers and pick the best.

A lot is at stake when it comes to NOC, especially around security measures, business continuity, and network management. You simply can't afford to hire a provider that doesn't adhere to the right NOC practices. In this document, we outline the ten important questions MSPs should ask prospective NOC service providers to be sure a large chunk of their business goes in 'able hands'.

1. Does the NOC provide 24x7 live telephone access to a qualified engineer?

A NOC is a centralized location where technicians directly support the efforts of remote monitoring, high-level security actions, and backup - disaster recovery. In a typically implemented network operations center, these technicians commonly are not available for live calls. Instead, they work behind the scenes and use an intermediary to handle communication. This can present a challenge when it comes to seamless and fluid communication. Despite this customary definition of a NOC, you can expect NOC techs to provide you with knowledgeable and real-time updates as well as perform double duty as helpdesk support when it's necessary. Make sure you know what you are getting into before you sign on the dotted line.

2. Does the NOC work in tiers or is it full incident management?

Some NOCs perform fault detection, troubleshooting, and tracking to identify and resolve network issues in different tiers. But those NOCs can often have a standard "run book" that they use to determine "in-scope" actions, then they send the ticket back to the customer. This may lead to unexpected overages in your bill. A full-service NOC should manage end-to-end remediation that includes support across the full IT stack (Wintel, networking, storage, virtualization, etc.), vendor coordination, and vendor escalation.

An incident management team, on the other hand, ensures an incident (an unplanned or undesired event that interrupts business operations) is closed or resolved within a predefined time limit described in a Service Level Agreement (SLA). Rather than working in tiers, the full incident management team creates a workaround solution to overcome the issue as quickly as possible so the affected network can continue operating normally.

3. Is the NOC SOC 2 Certified?

Having a SOC 2 certified service partner onboard means ensuring they securely manage your data to protect the interests of your organization and the privacy of your clients. For security-conscious businesses like MSPs, 'SOC 2 compliance' is a minimal requirement when considering a NOC.

4. Will the NOC sign BAAs for HIPAA clients?

How important this question is depends on your business. If HIPAA, PCI, or GDPR compliance is important, you need a service provider with the tools and certifications to deal with it. Check if the NOC service provider offers a service-level agreement (SLA) and a Business Associate Agreement (BAA) that guarantees the compliance you require. Mistakes are costly!

10 Exchange Place, 17th Floor
Jersey City, NJ 07302
Email: sales@itbd.net

5. Does the NOC have a detailed and comprehensive 'onboarding process'?

Onboarding, the process of incorporating a new service or solution into the existing environment of an MSP, can get quite tricky. Communicating with multiple vendors to ensure all the pieces of the puzzle fit together is just one part of the process. An expert NOC service provider should be able to make sure all hardware and software in use by the MSP and its customers are integrated. The entire process must also touch on essential processes such as incident management and escalation.

In an ideal scenario, the NOC service provider should start the onboarding process by meeting with your team to understand your goals, establish a timeline, gather data on your inventory, and verify the information. The provider should then compile all of the scenarios and responses into a single run book to assure all data points are correct. Only after this run book is extensively tested to ensure it works as intended, the service should go live.

6. Does the NOC perform quarterly business reviews or conduct bi-weekly or monthly service reviews?

In the age of automation and remote access, Quarterly Business Reviews (QBRs) are one of the best tools NOC service providers can use. In each QBR or biweekly/monthly review meeting, service providers broadly touch on a quick recap of big wins and losses, service ticket reviews, endpoint management, updates on user training, a report on the number of issues resolved, and infrastructural needs and goals for the future. Though QBRs are not about getting down into the nitty-gritty of daily operations, they are an opportunity for both parties to discuss strategy and results.

7. Does the NOC provide with a full team and a single point of contact?

While having access to each member of the NOC team has its own advantages, having a single point of contact (SPOC) brings discipline and consistency to the support process. Also, a SPOC model typically means lower costs.

A SPOC is not expected to resolve every ticket it logs. Rather, a SPOC is often a facilitator and coordinator of the entire end-user support process. He/she monitors the progress of all open tickets, prompting action on tickets that appear to be stalled, and closing tickets that have been resolved satisfactorily.

8. How does the NOC build efficiencies?

The answer to this question lies in a NOC’s structured operational processes. By building a table of escalation (to ensure all team members are clear on the proper protocol and channels for escalating issues) and understanding the prioritization of incidents in terms of their business impact can help build NOC efficiency. An ability to work on problem management alongside ongoing incident management (so ticket volume can be minimized) is what you should look for to ensure you’re selecting a proactive NOC.

9. Does the NOC provide detailed reporting?

Choose a NOC that creates reports on a daily and monthly basis. A daily report should include all major incidents of the past 24 hours and a root cause for each resolved incident. Detailed reporting by NOC also keeps your IT department and shift leaders informed about the NOC activities and of major incidents. Compiling these daily reports into a monthly report will help measure the team’s progress and reveal areas of improvement.

10 Exchange Place, 17th Floor
Jersey City, NJ 07302
Email: sales@itbd.net

10. What is the NOC escalation path?

A high escalation rate indicates clients are not pleased with the resolution at the SPOC level as they want someone at a higher level within the NOC to resolve the complaint. To maintain a reasonable escalation path, a table of escalation should be maintained to ensure that all team members are clear on the proper protocol and channels for escalating issues. A critical problem that was not solved within 30 minutes should be escalated up the management ladder until response and/or ownership is taken.

In closing:

An outsourced NOC should offer your MSP a competitive advantage. Perhaps it is cost savings, perhaps it is better utilization of your in-house engineers, perhaps it is support for a particularly needy client. But without properly vetting your choice, the exact opposite can happen.