S/No 10.3	Compliance Network Management System (NMS)	Yes/No	Remarks
1	NMS shall be able to monitor and configure **500** devices (should be proposed against the proposed devices) and should have scalability to manage up to **2000** devices in future. NMS shall be able to manage both **wired** (routing/switching) and **wireless** networks in **single pane of glass** management.	Yes	
2	NMS should be scalable to provide Deep application visibility using AVC, NetFlow/Sflow, NBAR or packet inspection to recognize a wide variety of applications and SNMP.NMS should be able to provide Network topology.	Yes	
3	NMS solution should deliver pinpoint visibility into who, what, when, where, and how of wireless access through its own data collection and key integrations. It should support spatial / floor mapping; integrated location- based tracking of client	Partial	**real time user movement is not covered.** **Defined Location based dynamic integration is enabled.**
4	Should provide a customizable at-a-glance summary of all discovered devices and existing network switches to proactively identify problem areas and help prevent network downtime. The network has to be manageable at Network Operations Center (NOC) and through secured browser.	Yes	
5	Should be able to discover, configure, monitor, manage, and deploy configurations to dynamically update groups of devices.	Yes	
6	Should allow flexible definitions of administrator roles and responsibilities with RBAC (Role based Access Control) for different teams.	Yes	
7	Should enable performance management by providing customizable dashboards and historical data visibility	Yes	
8	Should be able to generate reports designed to summarize utilization of and traffic patterns on network interfaces.	Yes	
9	Should allow administrators to track device configuration changes, enabling viewing, retrieval, and restoration of configuration files, and monitoring of configuration drift for troubleshooting purposes.	Yes	
10	The system design should provide access to only authorized users, RBAC and by using Secure Digital Certificates to completely trace back an individual user, in case of Cyber Crime or any other cyber investigation, as per the Computer Assets and Information Technology (CAIT) Policy of PATNA Hospital.	Yes	**FCAPS, ITSM, ITILv3 Supported.** **Kindly share policy CAIT document**
11	Should have direct OEM 24x7x365 TAC support with software upgrade and NBD Advanced hardware replacement warranty for 5 Years.	Yes	