SIG-NOC Tools Survey

What software tools R&E Network Operations Centres use

June 2016

Table of Contents

1. Introduction

The Special Interest Group – Network Operations Centres (SIG-NOC) is a community effort [1] initiated by the National Research and Education Network organisations (NRENs) gathered under the GÉANT association in Europe. SIG-NOC creates an open forum where experts from the GÉANT Community and beyond exchange information, knowledge, ideas and best practices about specific technical or other areas of business relevant to the research and education networking community. SIG-NOC is the successor of the former TERENA Task Force on NOCs (TF-NOC).

TF-NOC completed and published its first 'NOC Survey' by December 2011 [2]. That survey had a wider scope covering the NOCs' taxonomy, structures, resources, tools and other aspects. Towards the end of 2015, SIG-NOC decided to repeat only the NOC tools related part, because it was realised that the tools and techniques used by the NOCs had progressed a lot since the last survey.

In the second 'NOC Tools Survey' covered in this report, information about the software tools that NOCs use to operate networks and services was collected between December 2015 and February 2016. One section was dedicated to the adoption of standards and industry best practices as well as training activities.

Since the survey was mainly focusing on tools and operation practices it was recommended to be filled out by someone who has an overview of the whole NOC's operations.

The results of the survey are summarised in this report. The anonymised survey data is also available on the SIG-NOC home page [1] in MS Excel format (i.e. raw data and zoomable graphs) for further analysis.

2. Survey Participants

We received 78 individual responses to the survey of which 64 were valid and fully or partly complete. It represents a much better turn out compared to the first survey in 2011, where we were able to analyse only 43 responses.

Chart 1 shows the type and range of networks that participated in the survey. We got more coverage in each category. This is partly due to the fact that the SIG-NOC group has been growing and able to reach out to more operators, but it could also be caused by the fact that the same NOCs are covering more and more networks, services and functionalities. The numbers of national research and education networks, campus networks, and Internet Exchanges clearly stand out, compared to the results in 2011.

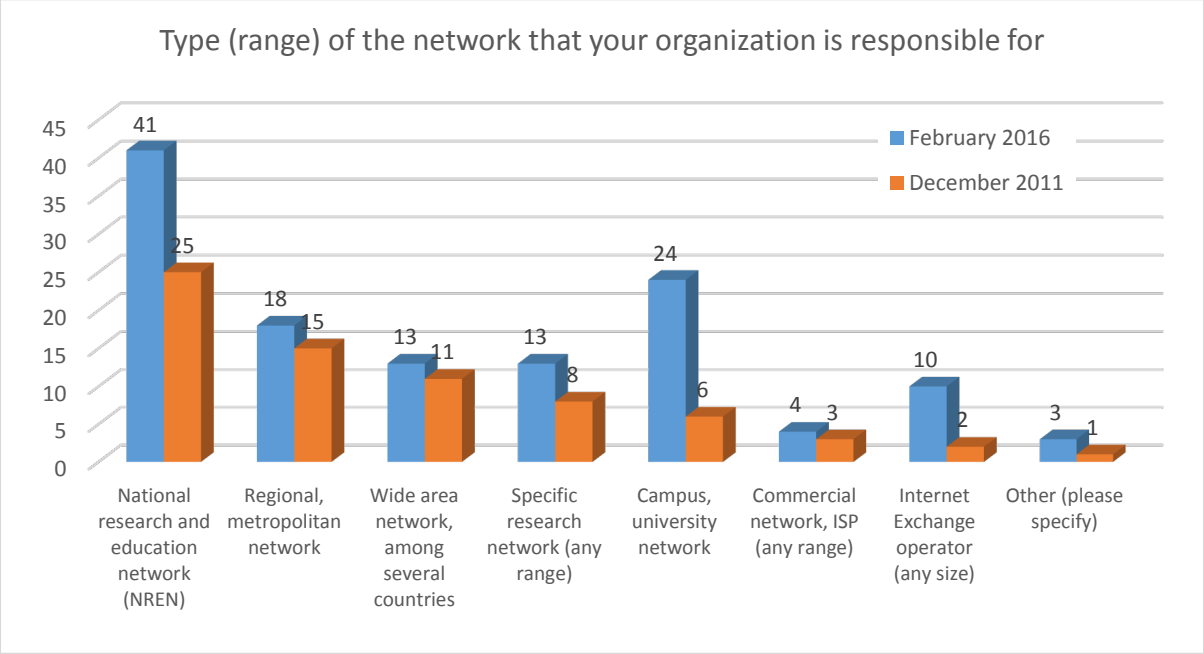

Chart 1. Type (range) of networks answering the survey

In 2016, the other category included datacentre, cross-border fibre and e-government network operators as special types.

3. NOC Functions

The survey covered 15 functions that the NOCs may be responsible for. *Table 1* lists all the functions in the order of their importance as rated by the respondents. In comparison to 2011, the relevance of problem management, performance management, configuration management, change management and DDoS mitigations have grown significantly. The importance of monitoring stayed constantly high, while resources management is often covered outside of the NOCs.

December 2011	February 2016	Trend
Monitoring	Monitoring	0
Ticketing	**Problem Management**	+5
Reporting and Statistics	Ticketing	-1
Communication, Coordination and Chat	**Performance Management**	+4
Knowledge Management and Documentation	Reporting and Statistics	-2
Out-of-band Access Management	**Configuration Management and Backup**	+3
Problem Management	Communication, Coordination and Chat	-3
Performance Management	Knowledge Management and Documentation	-3
Configuration Management and Backup	**Change Management**	+3
Inventory Management	Out-of-band Access Management	-4

Security Management	Security Management	0
Change Management	Inventory Management	-2
Data Aggregation, Representation, Visualization	**DDoS Mitigation**	+2
Resources Management	Resources Management	0
DDoS Mitigation	Data Aggregation, Representation, Visualisation	-2

Table 1. Comparison of NOC functions

The 2015 data is also depicted in *Chart 2*. The functions in the first 9 columns (from monitoring to change management) are covered by more than 60% of the NOCs that responded to the survey.

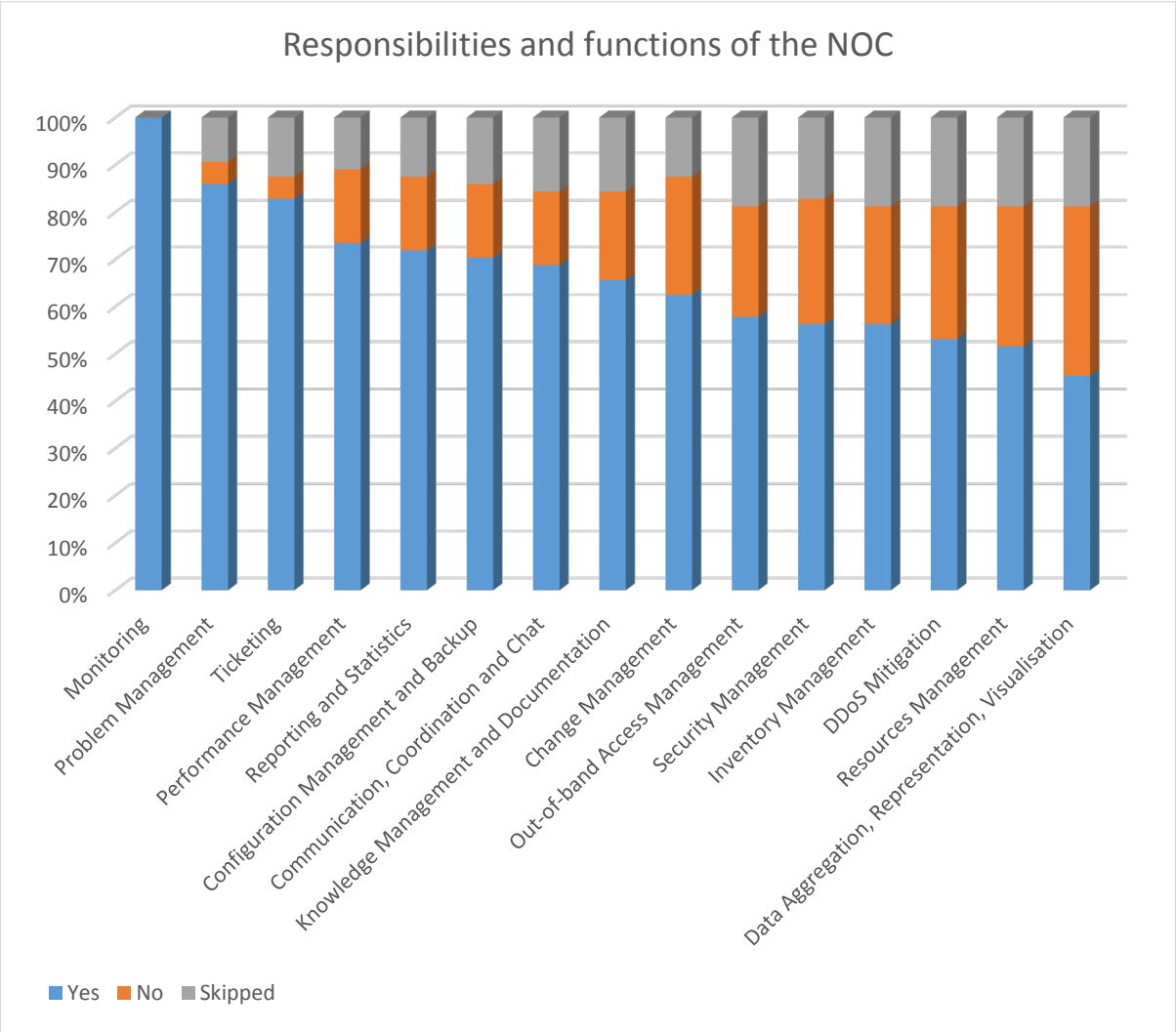

Chart 2. NOCs responsible for the particular functions

4. NOC Tools

In this chapter, the various software tools used to fulfil the particular functions are shown rated by their importance and quality: horizontally the importance, vertically the ratings are depicted. The larger the circle the more the answers that we got regarding the particular tool. The smaller circles represent some tools that may be below or above average, but bear in mind that this is based on the opinion of a smaller set of respondents only. We suggest to take into account the bigger circles or the ones with the same/similar relative sizes in any comparison.

4.1. Monitoring

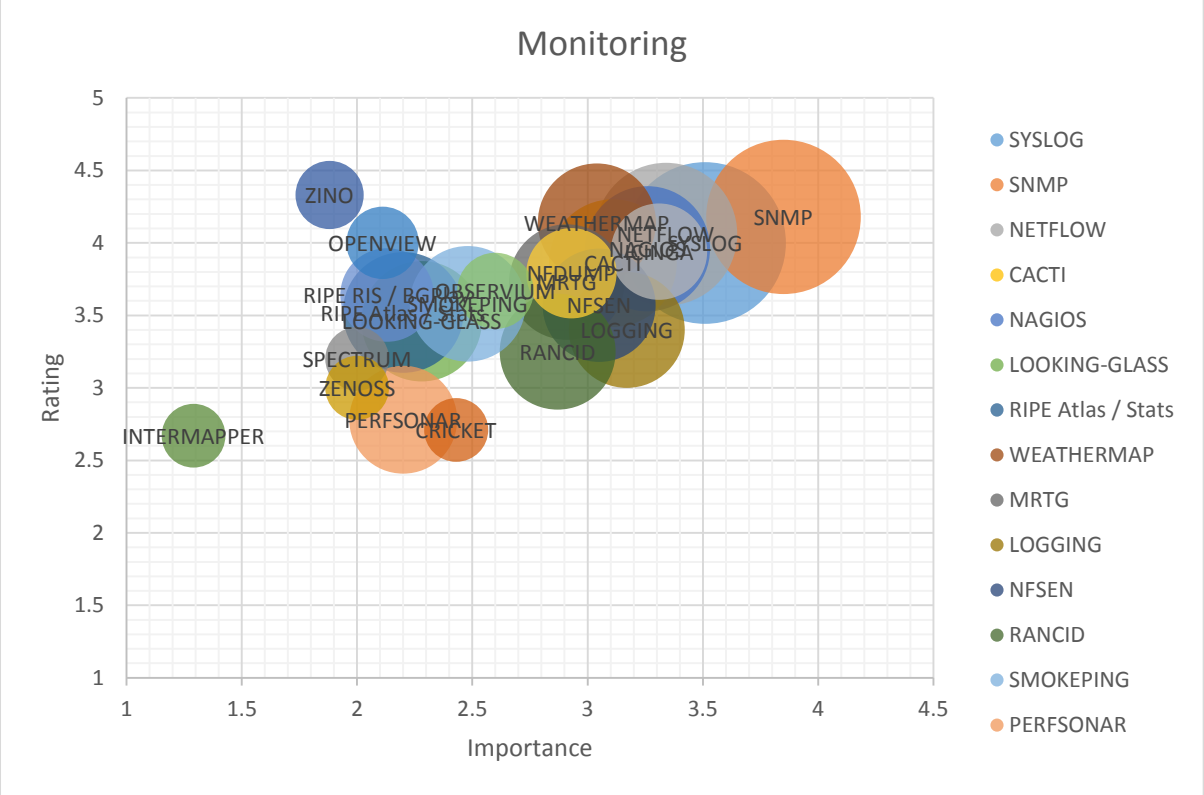

Chart 3. Software tools used for monitoring

SYSLOG is the preferred way to gather the information from the equipment, closely followed by SNMP and NETFLOW. The best rated tools are the same as in 2011: CACTI and NAGIOS. ZINO has got a high rating but its importance is less and it is not used by that many NOCs. For instance, PERFSONAR and RIPE Atlas are in the same size and importance, and the quality of the later is rated higher by the NOCs.

Table 2 below lists some of the other tools and in-house developed solutions not included in the survey.

Other tools:	• Zabbix (4) • Munin (3) • CheckMK (2) • AS-Stats • LibreNMS • CENTREON • Swatch • Ciena OneControl • IBM Tivoli • NAV • Netdisco • Net-minder • Speedtest • Puppet • Racktables • Patchmanager • Splunk • Network Polygraph • NMS from DWDM vendors
In-house developed solutions:	• GINS (GARR Integrated Networking Suite) • minemon (ICMP and BGP session checks, perl-based) • NAV developed by UNINETT • Rancid frontend • MRTG front-end, Netflow analyser • Service availability overview: RRDtool • FTAS, G3 by CESNET • SMARTxAC • Turbo Krt • Vialpe: a distributed cacti+smokeping on a georeferenced interface by RNP

Table 2. Other tools and in-house developed solutions for monitoring

4.2. Problem Management

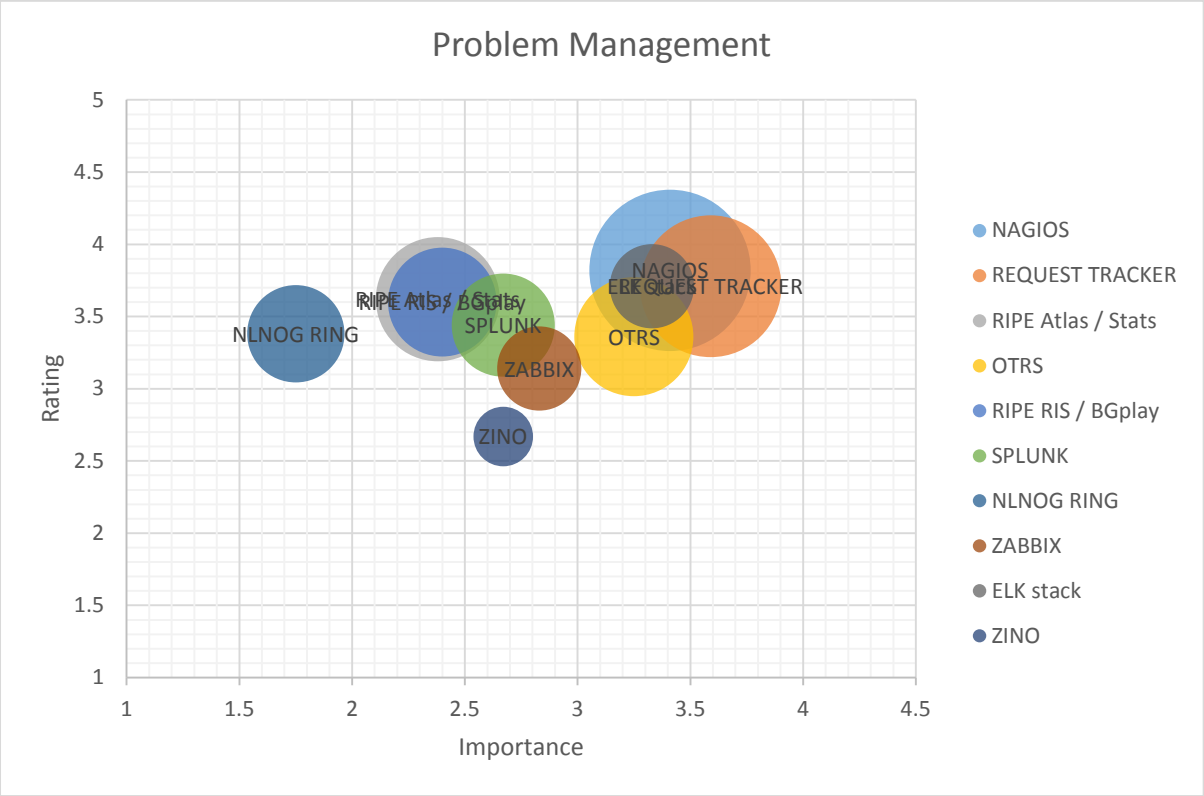

Chart 4. Software tools used for problem management

NAGIOS, REQUEST TRACKER and ELK Stack are rated the highest with relatively high importance although ELK Stack is not used by that many NOCs. There are a few good tools that are useful for problem management but less important, such as RIPE Atlas and RIPE RIS/BGplay.

Other tools:	• JIRA (3) • Kibana • HP Openview • SpiceWorks • Observium • Munin
In-house developed solutions:	• TTS • Syslog-analyzer, alarm features on CheckMK and MRTG • GN6, based on Ofbiz • RT integration with Zenoss and Customer - link database

Table 3. Other tools and in-house developed solutions for problem management

4.3. Ticketing

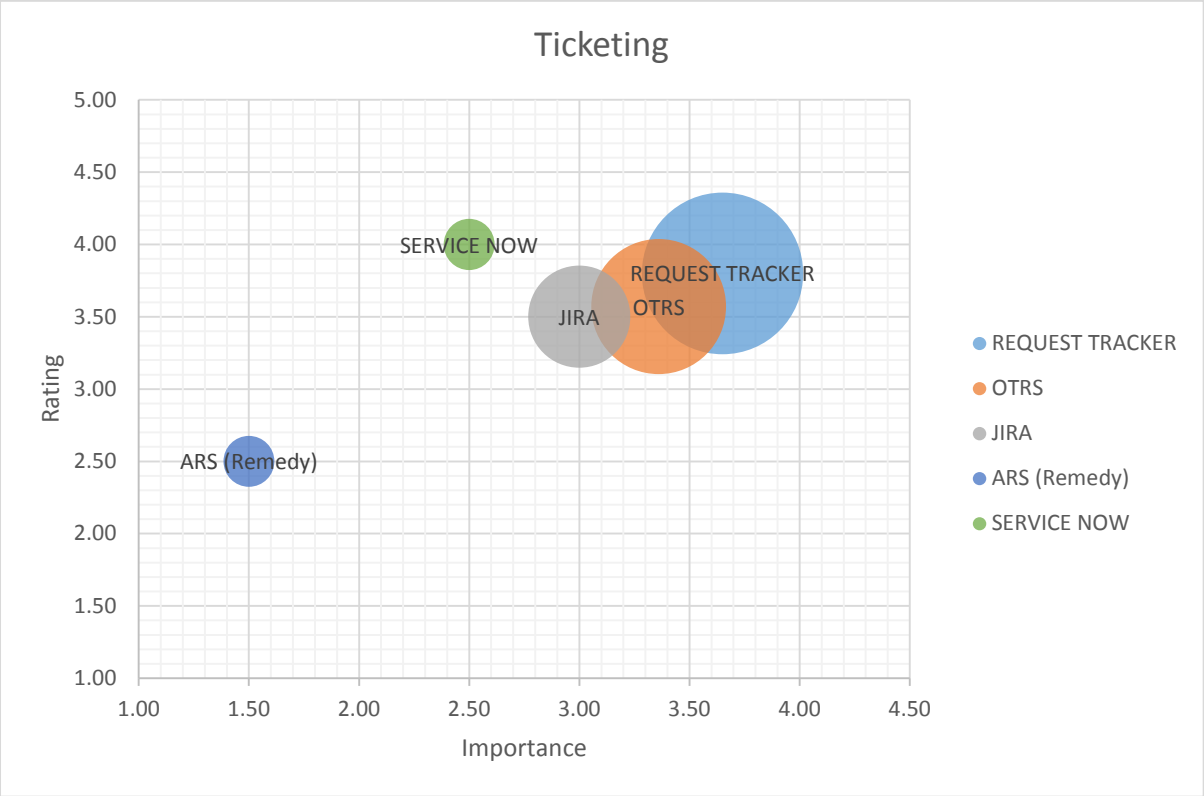

Chart 5. Software tools used for ticketing

REQEST TRACKER, OTRS and JIRA are in this exact order in terms of importance, quality and use. SERVICE NOW is rated highly, but only in a small sample and it's not primarily for ticketing.

Other tools:	• MANTIS Bug Tracker • TRAC • HP Openview Service Desk • VC4 IMS • Clocking • SpiceWorks • GLPI
In-house developed solutions:	• TTS (2) • GN6, based on OfBiz • ticketing for drupal

Table 4. Other tools and in-house developed solutions for ticketing

4.4. Performance Management

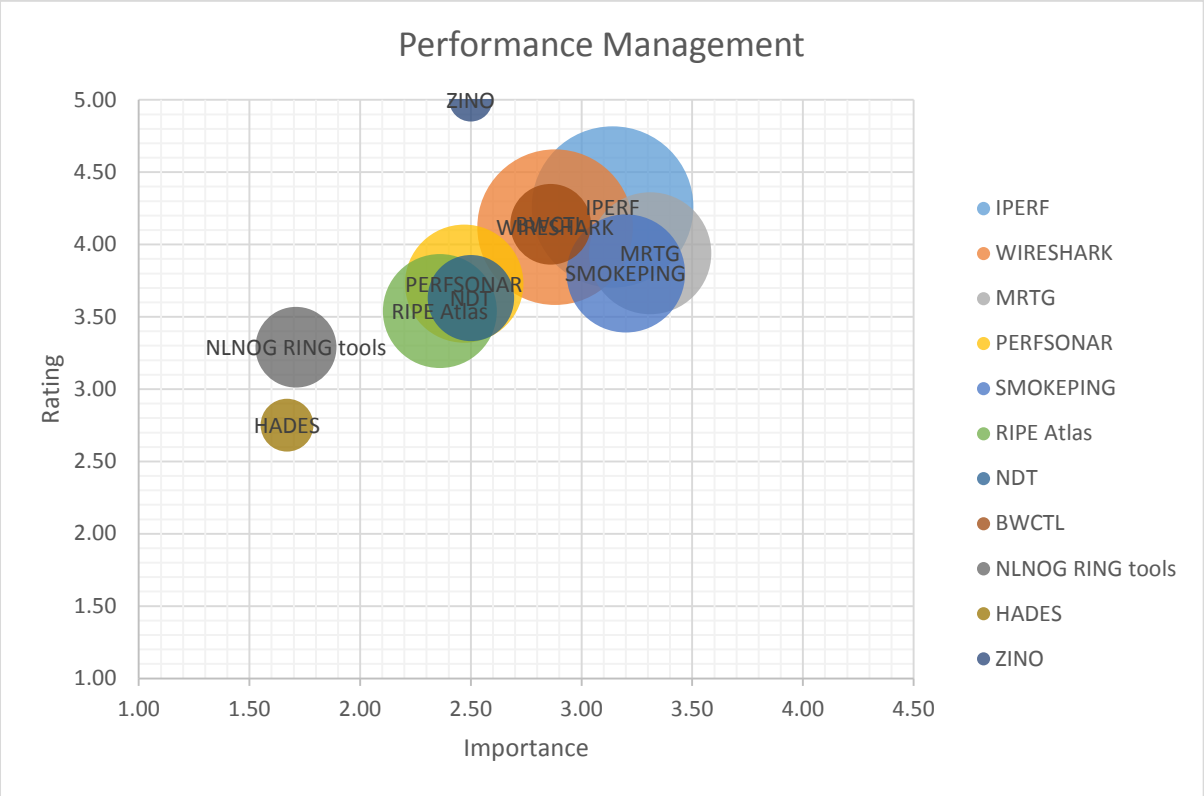

Chart 6. Software tools used for performance management

IPERF, WIRESHARK, MRTG and SMOKEPING are the most important tools. ZINO has got a high rating but only on a small sample.

Other tools:	• Mgen (2) • RRD • Spirent appliances • Speedtest • NAV
In-house developed solutions:	• BWM, Live BWM by CARnet • Threshold alarming in MRTG and CheckMK

Table 5. Other tools and in-house developed solutions for performance management

4.5. Reporting and Statistics

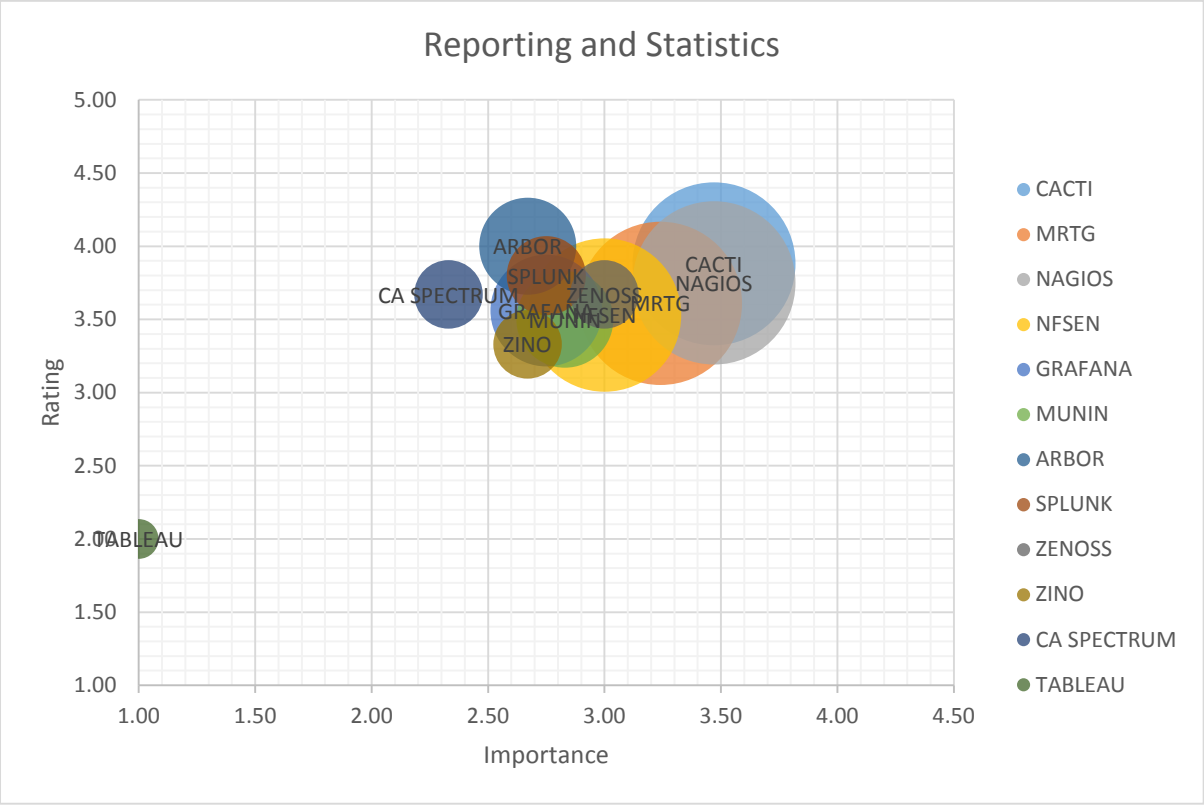

Chart 7. Software tools used for reporting and statistics

CACTI, NAGIOS and MRTG stand out, but most of the tools are very close to each other in terms of importance and quality.

Other tools:	• RequestTracker (2) • Zabbix (2) • Kibana • LibreNMS • Torrus • RRDtool • infovista • sanet • Grafana is included in NAV, NFDump and manual analysis
In-house developed solutions:	• GINS • SNMP stats export, Netflow stats • Pinger tool with added extensions, Nagios extensions

Table 6. Other tools and in-house developed solutions for reporting and statistics

4.6. Configuration Management and Backup

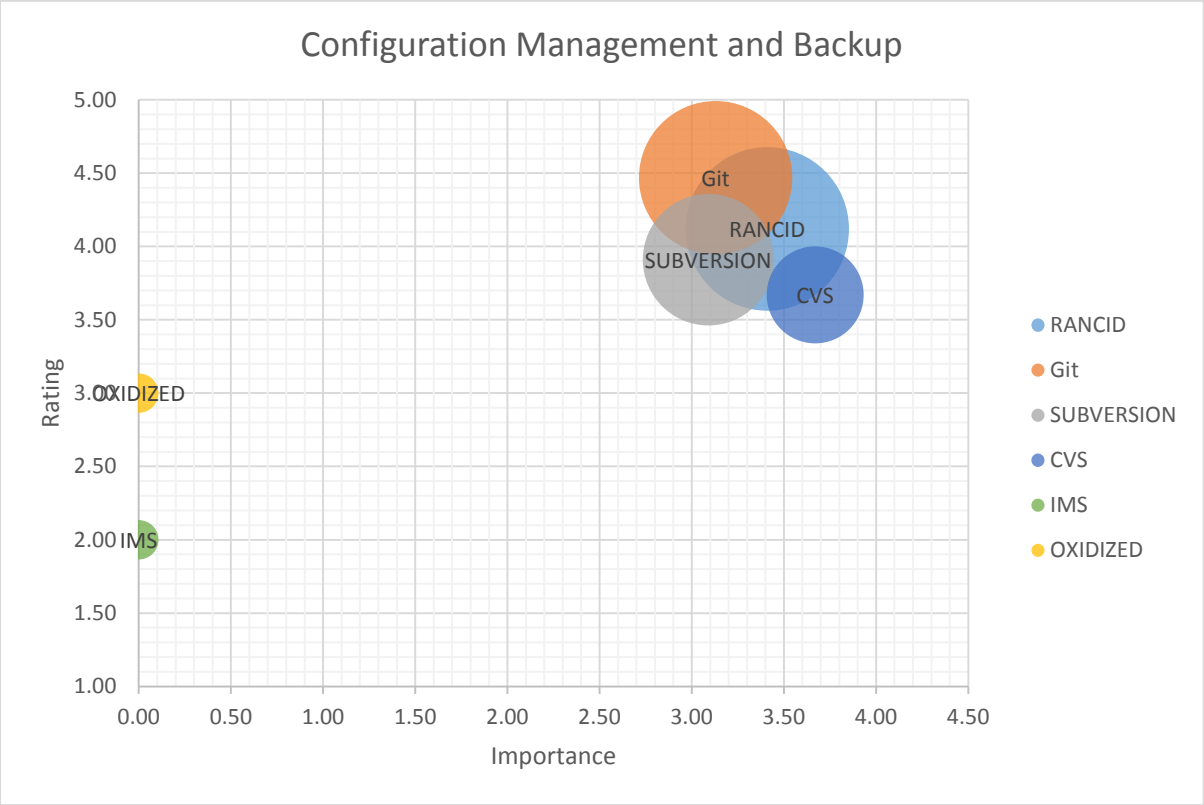

Chart 8. Software tools used for configuration management and backup

Git, RANCID, SUBVERSION and CVS are the popular tools, the others were not rated as important.

Other tools:	• RCS (4) • CA Spectrum and FTP server • Puppet • Backuppc • etckeeper • Racktables • Patchmanager • Ciena NMS • SCCS • veeam • imc
In-house developed solutions:	• Rancid-like tools • GN6, based on OfBiz

Table 7. Other tools and in-house developed solutions for configuration management and backup

4.7. Communication, Coordination and Chat

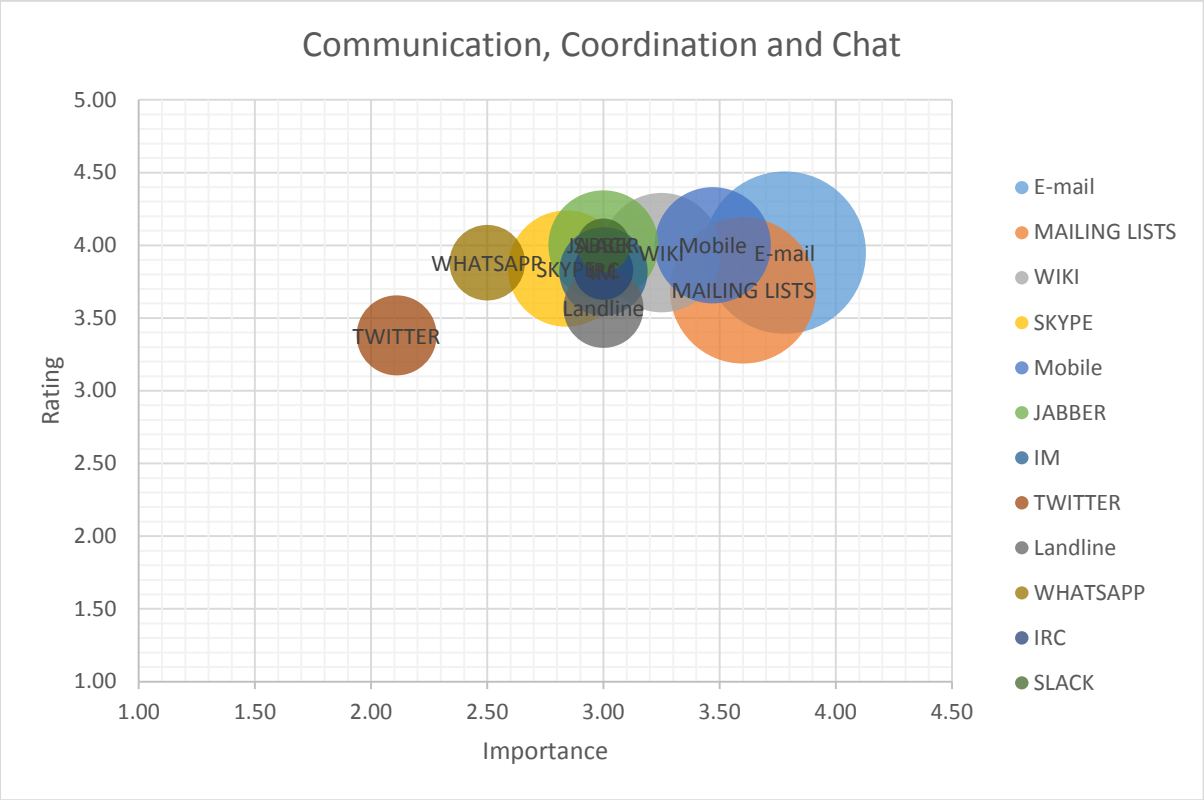

Chart 9. Software tools used for communication, coordination and chat

Interestingly traditional communication and new social tools are considered almost equally good. However, e-mail, mailing lists and mobile phone are still the most important tools.

Other tools:	• Asterisk • Kamailio • CalDav • ServiceInfo (webbased sender for mailing lists) • SharePoint
In-house developed solutions:	• N/A

Table 8. Other tools and in-house developed solutions for communication, coordination and chat

4.8. Knowledge Management and Documentation

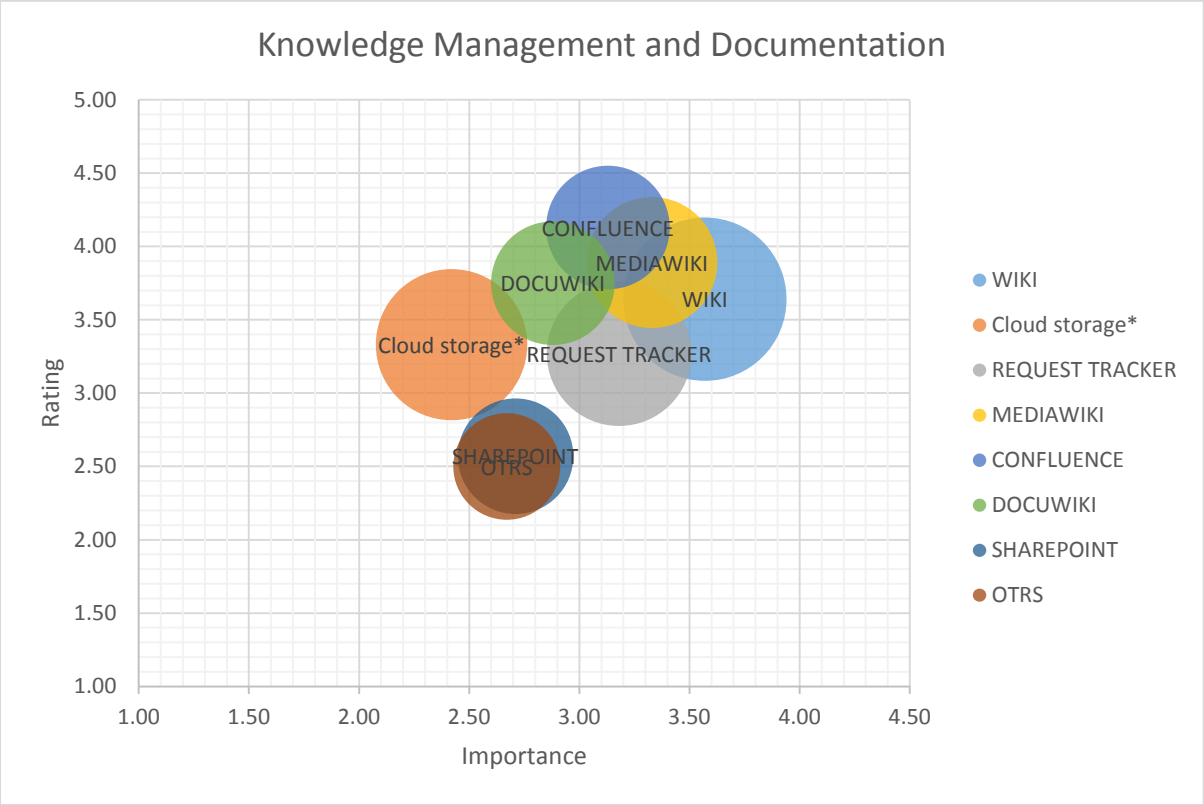

Chart 10. Software tools used for knowledge management and documentation

Wiki platforms are considered the best for many users. Confluence has go the highest rating with slightly less users. Different cloud storage solutions are used by many NOCs, but their importance is relatively low.

Other tools:	• MoinMoin Wiki • TRACwiki • TiddlyWiki • FosWiki • Drupal CMS • File server	• Subversion • Plone • ownCloud • SURFdrive • OneDrive
In-house developed solutions:	• Home-grown inventory / CMDB system (KIND) • Database (GIS) • Comunitats, based on Plone	

Table 9. Other tools and in-house developed solutions for knowledge management and documentation

4.9. Change Management

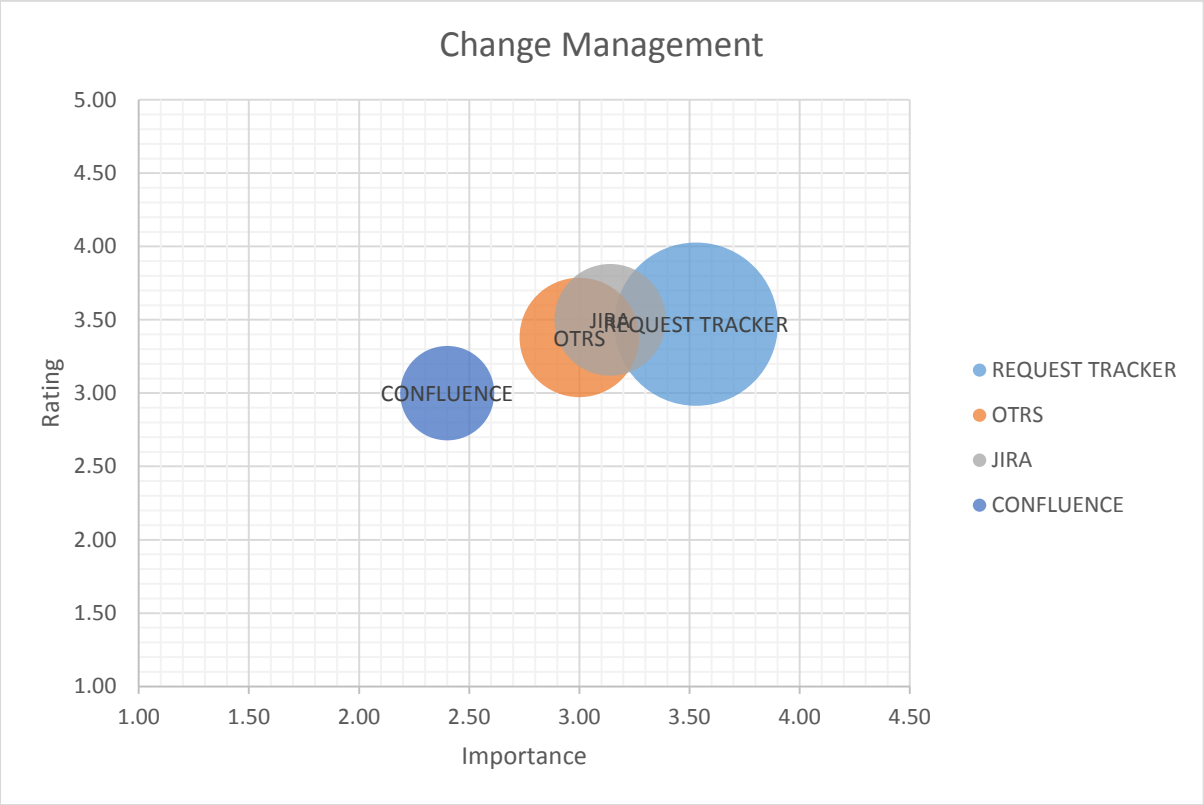

Chart 11. Software tools used for change management

REQUEST TRACKER is the most important and highly used tool for change management followed by JIRA and OTRS.

Other tools:	• Redmine • gitlab • Racktables • Patchmanager • HP Openview Service Desk
In-house developed solutions:	• pymetric • Wiki • GN6, based on OfBiz • In house Change Request generator • ticketing for drupal

Table 10. Other tools and in-house developed solutions for change management

4.10. Out-of-band Access Management

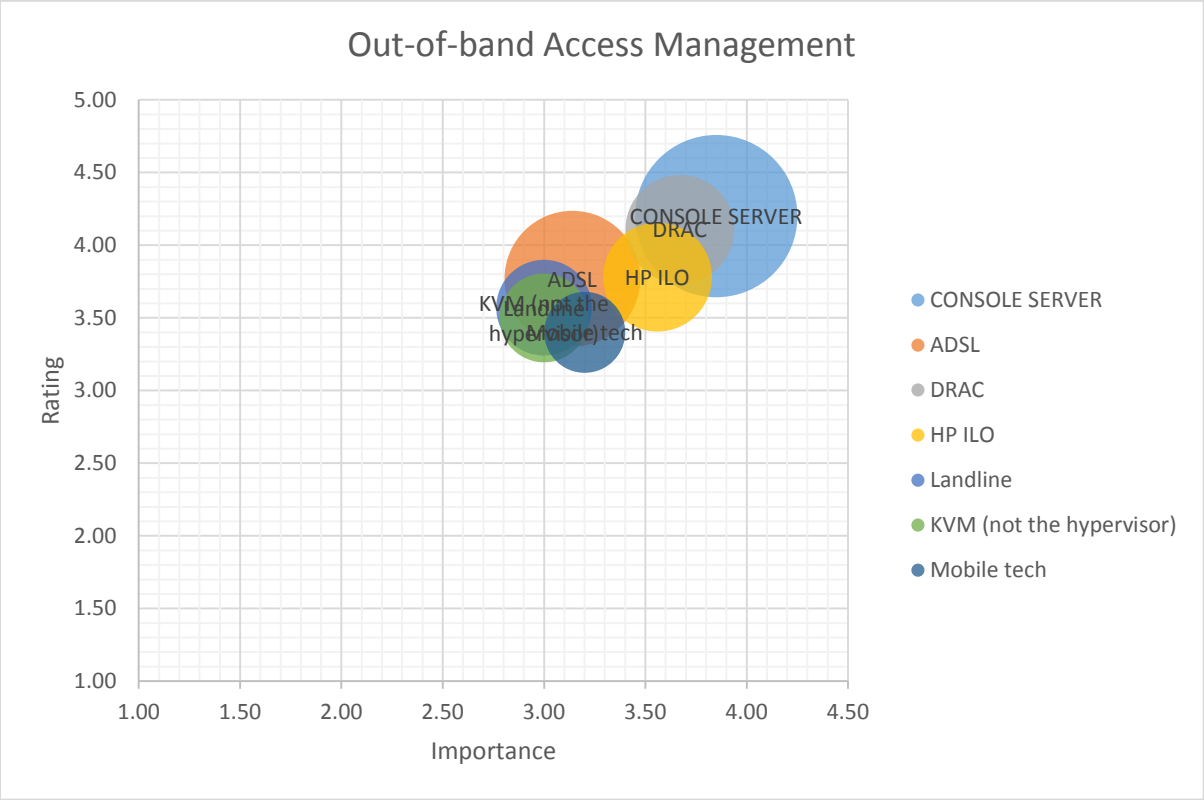

Chart 12. Software tools used for out-of-band access management

CONSOLE SERVER is felt to be the most highly rated and important solution.

Other tools:	• ISDN (2) • DWDM OSC • we currently use POTS for access, but want to move away from that
In-house developed solutions:	• N/A

Table 11. Other tools and in-house developed solutions for out-of-band access

4.11. Security Management

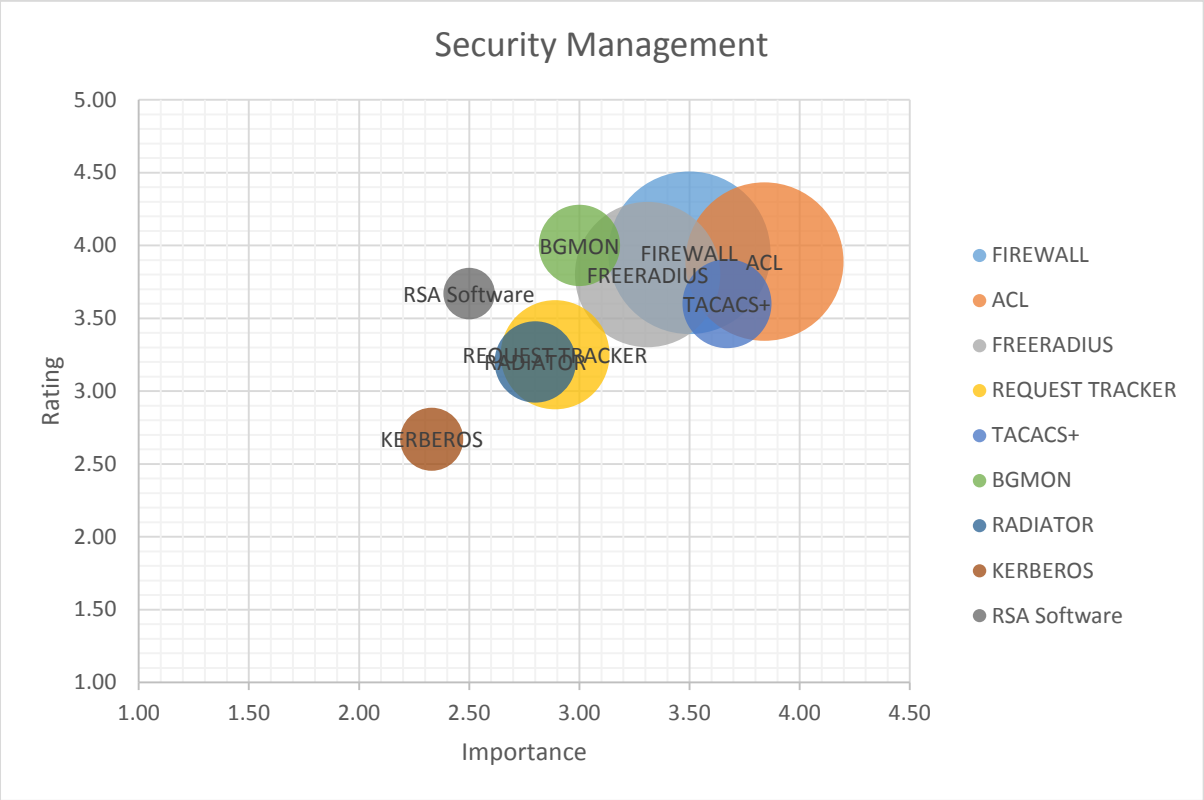

Chart 13. Software tools used for security management

Firewalls and ACLs are used by almost all the institutions who answered this question. BGPmon is highly rated, but not used by so many NOCs.

Other tools:	• FirewallBuilder (2) • RTIR • Netflow analyzer
In-house developed solutions:	• N/A

Table 12. Other tools and in-house developed solutions for security management

4.12. Inventory Management

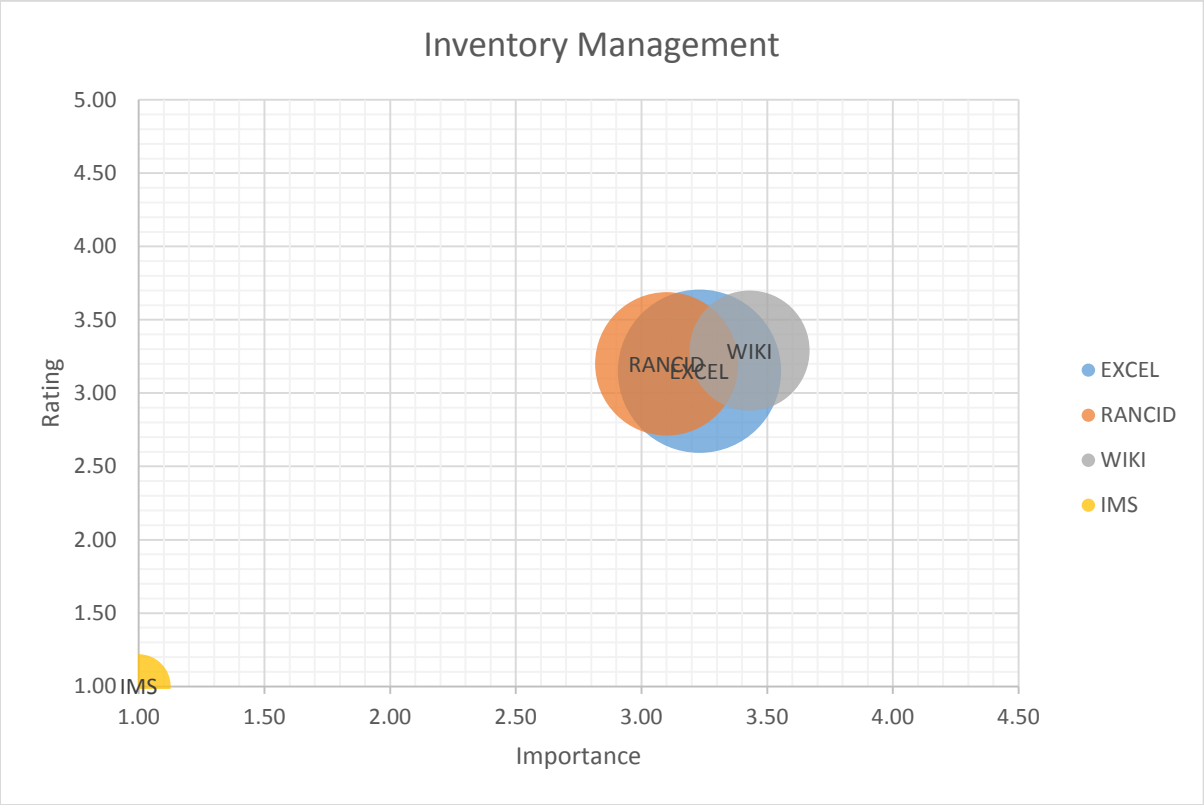

Chart 14. Software tools used for inventory management

Almost all the listed tools are in the same quality and importance range however not primarily designed for proper inventory management. Better tools are listed in *Table 13*.

Other tools:	• RackTables (2) • IIR (2) • Patchmanager • HP Openview Service Desk • HP Openview NNM	• Ciena NMS • filemaker • netdisco • Observium
In-house developed solutions:	• KIND (home-grown inventory/ CMDB) • In-house developed tool based on SNMP, RANCID, Apache & MySQL • CMT • GarrDB • MySQL + Perl + lots of text • GIS Database	• inventory PHP based • GN6, based on OfBiz • home-grown database-application • Asset Database • Grejp • own database tool

Table 13. Other tools and in-house developed solutions for inventory management

4.13. DDoS Mitigation

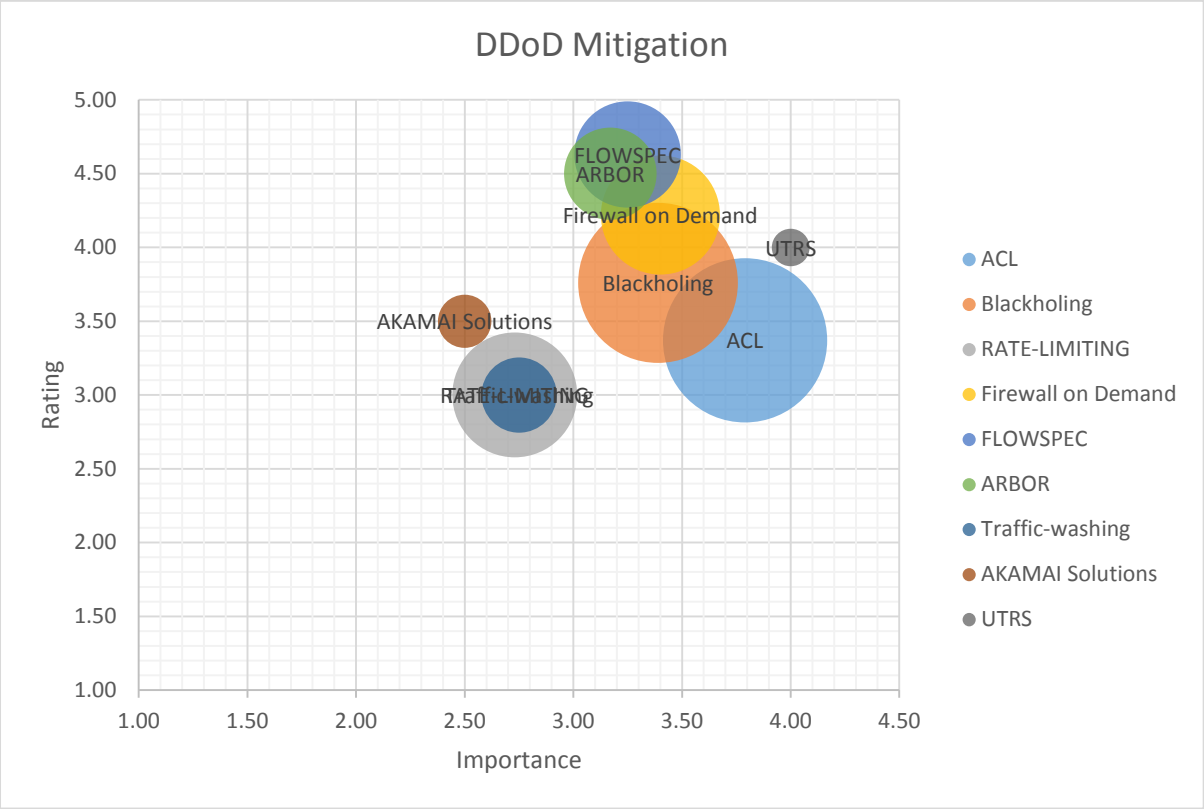

Chart 15. Software tools used for DDoS mitigation

FLOWSPEC, ARBOR and Firewall on Demand are highly rated tools in general, but most of the NOCs use Blackholing and ACLs.

Other tools:	• Fastnetmon
In-house developed solutions:	• DDoS detection and traffic washers

Table 14. Other tools and in-house developed solutions for DDoS mitigations

4.14. Resources Management

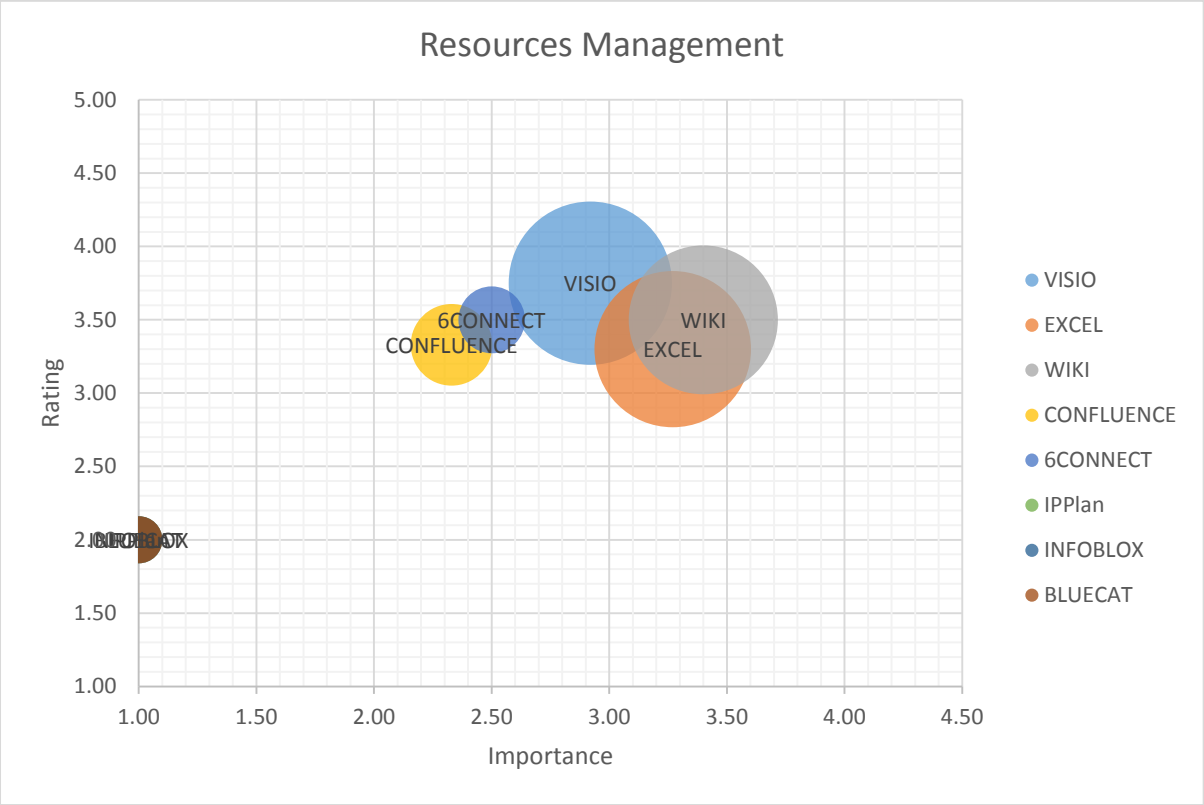

Chart 16. Software tools used for resources management

VISO, Wiki and Excel are the commonly used tools for resources management although this function is often considered outside the remit of the NOC.

Other tools:	• Racktables (4) • omnigraffle (2) • Commercial GIS application • vi, flat files, rcs, scripts • Network Inventory	• Plaintext-files • GestioIP • HP Openview Service Desk • phpipam
In-house developed solutions:	• KIND (home-grown inventory/ CMDB) • Web pages using PHP • IPAM • Resources Management: Web-based list of networks and router-interfaces	• GIS Database • BDcom database • home-grown database application

Table 15. Other tools and in-house developed solutions for inventory management

4.15. Data Aggregation, Representation and Visualisation

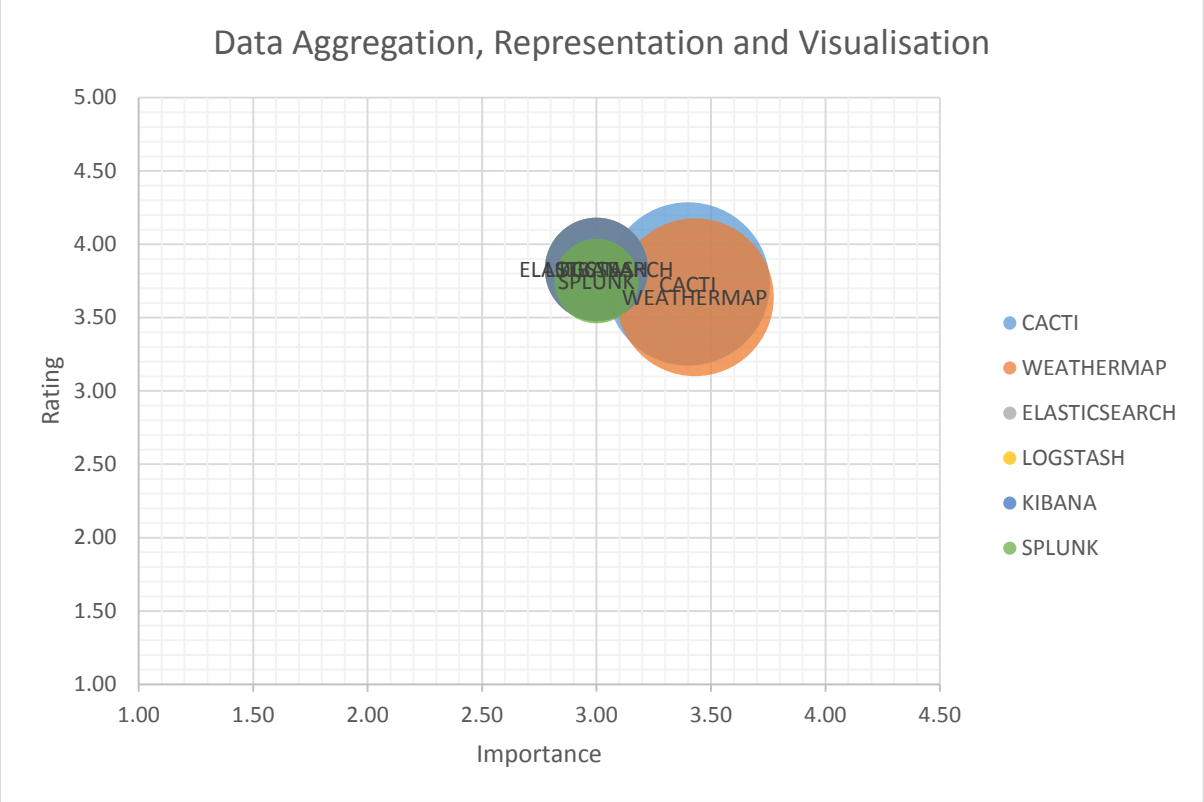

Chart 17. Software tools used for data aggregation, representation and visualisation

CACTI, WEATHERMAP and ELASTICSEARCH are the most important tools: their qualities are almost the same.

Other tools:	• MRTG, Tivoli maps, Juniper RIM • Zino • Zenoss • CheckMK • Observium
In-house developed solutions:	• N/A

Table 16. Other tools and in-house developed solutions for data aggregation, representation and visualisation

5. Standards and trainings

As part of the survey, SIG-NOC wanted to figure out the level of adoption by the NOCs of the various standards and industry best practice-based procedures and methodologies. These results will serve as an input to the NOC training development exercise that SIG-NOC intends to carry out later in 2016.

Chart 18 shows the various standard adoptions. The ISO 27001 Information Security Management standard has been implemented by 23.5% of the respondents somewhere in 60 to 100% completeness. On the other hand, 47% of the respondents have not yet started implementing ISO 27001 standard at all. ISO 27000 is part of a growing family of ISO/IEC Information Security Management Systems (ISMS) standards, but its level of adoptions is not that significant. ITIL is not a standard but a set of industry best practices therefore it provides some room for implementation that is happening at many NOCs. About 80% of NOCs started to comply with ITIL recommendations, about one third of them are in 5 to 30% and another one third of them are in 30 to 60%. It represents a real take up and transitional path towards ITIL based operations.

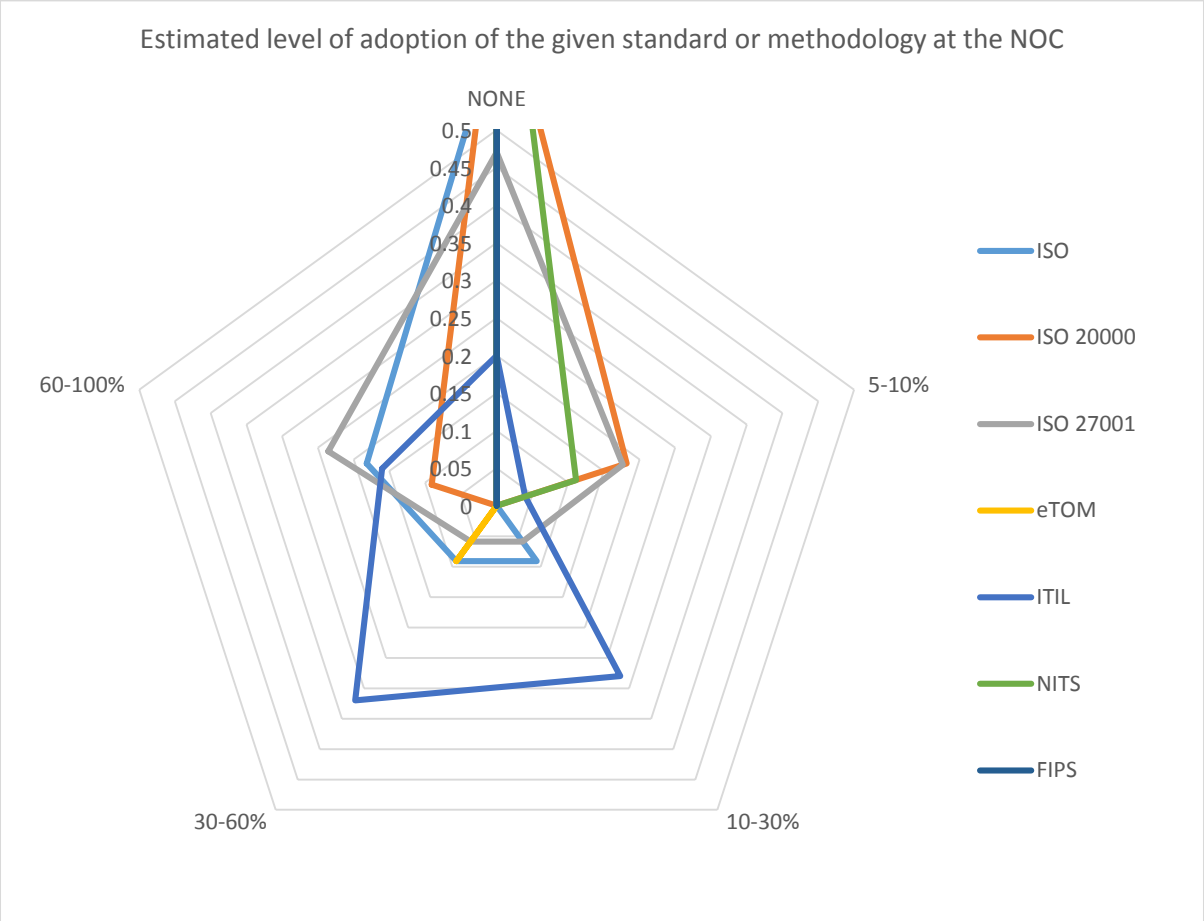

Chart 18. Estimated level of adoption of the given standards and methodologies

There was a question about the various internal trainings that the NOCs offer to their employees.

Regarding the same set of standards and methodologies above, ITIL training yet again stands out a little, but in general it can be seen on *Chart 19* that an 'average' NOC person is not necessarily certified or trained fully to understand all the context and details of these standards and methodologies. They are just expected to follow the procedures relevant to them.

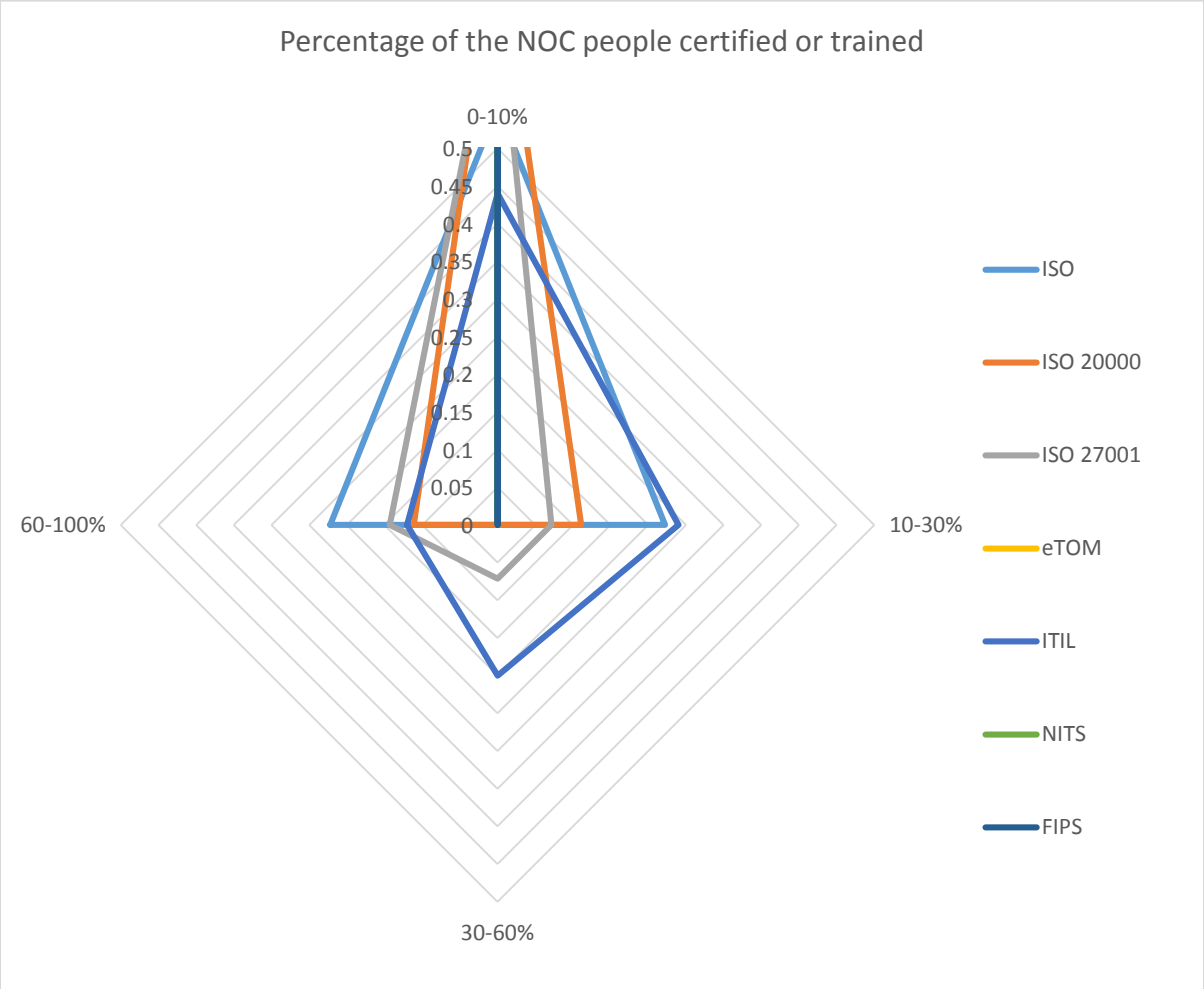

Chart 19. Percentage of NOC people certified or trained

In conclusion, it can be said that there is an opportunity for SIG-NOC to develop a training programme primarily based on ITIL best practices that can be extended and applied to specific NREN NOC scenarios and provide that training to the GÉANT NOC community and beyond.

The various training opportunities provided by NOCs to their people are listed in *Table 17*.

General/Procedural trainings	• Seminars, improvement courses
	• Mixed in-house training
	• Transmission training
	• Crisis and communication training
	• On the job training
	• General technical training: Coursera MOOC
	• We train our NOC members by:
	  ○ having generic documentation
	  ○ having specific documentation for our networks and/or customers
	  ○ going on site to work with them
	  ○ letting them come to our site for them to work with us
	  ○ inviting them when the NREN technical staff is trained for a product / technology that is useful for the NOC
	• Internal procedures walkthrough and working together with an older member ('shadowing')
	• Initial training to practical NOC duties.
	• In-house training on relevant topics at random intervals (rarely)
	• In-house. Many procedures are described in Dokuwiki and the rest is practice.
	• ITIL foundations
	• Network Auditing
	• English language training
	• Basic, in house, NOC training. Fibre safety. Data centre design/management. Troubleshooting.
	• No standard trainings. Most is learning by doing with the background of long-year experience with most of the staff-members.

Tool/Technology specific trainings	• Usually training on the job from the vendor when installing new equipment; in-house studies and workshops • DWDM / optical management • Juniper training • Vendor related training: Juniper, Fortigate, Cumulus • Dedicated courses on specific equipment (for instance Alcatel, Cisco, etc.), CCNA, Linux certification LPIC, RIPE NCC trainings • CCNA, CCNP, MikroTik academy, different in-house trainings • We do attend Juniper/Cisco/Alcatel education when appropriate

Table 17. List of training opportunities that NOCs provide to their people

6. Conclusions

As is evident, the range of tools in use across the NOCs who responded the survey is extremely wide. This report explicitly does not attempt to draw any conclusions on which tools are best. However it should be helpful in determining which tools are most commonly used and therefore likely have a healthy community around them. It also illustrates situations where tools are widely used, but perhaps not as widely found to be useful.

While further conclusions are left to the reader; should this survey report raise any questions with you, then please engage with the SIG-NOC community [1] to find discussion and answers.

7. Acknowledgement

SIG-NOC acknowledges the contributions of all the organisations and their NOCs who participated in the survey and extends its special thanks to the SIG-NOC Steering Committee members: Brian Nisbet (HEAnet), Maria Isabel Gandía Carriedo (CSUC), Jonny Lundin (NORDUnet) and Pieter Hanssens (Belnet).

8. References

[1] GÉANT SIG-NOC home page https://wiki.geant.org/display/SIGNOC/

[2] First NOC Survey 2012 https://www.terena.org/activities/tf-noc/survey.html

www.geant.org