Daisy Professional Services
Data Sheet

Network Assessment services

Information networks are arguably your most important IT assets, their speed and reliability are the foundations upon which your critical business systems and applications run. Ensuring your network infrastructure is available and performing to its optimum is a continual challenge.

This challenge however is one that is growing and increasing in pace driven by many factors such as:

- Massive growth in data volume, requiring processing and storage, and distribution over your network
- Convergence of voice, video and data traffic with IP telephony, peer to peer applications, video conferencing, and desktop collaboration technologies all requiring bandwidth with low latency
- Application and server virtualisation, leading to significant changes in traffic flows and patterns over the network with potentially 'bursty' application streaming traffic
- Desktop virtualisation. Server-side desktop virtualisation relies on an 'always-on' network and the user experience is very sensitive to bandwidth and network latency, whilst client-side desktop virtualisation involves 'bursty' and bulky streaming traffic
- Mobile devices – the prevalence of smart phones and tablets, and mobile applications means changes to how and where business data is delivered. Many wireless networks weren't designed for the 'new demand' – the number of connections, and the bandwidth requirements
- Workforce decentralisation to support flexible working, or deploying workers close to the 'work-flow' and to customers, means that secure remote network access becomes an essential ingredient to the efficiency of increasingly distributed staff

Maintaining the 'status quo' with consistently high network availability has always been a challenge in its own right, but with the pace of change and complexity steadily increasing, it merits a formal, structured, and regular review process.

Daisy's comprehensive range of Network Assessment services provides you with a detailed understanding of:

- Your current network assets and architecture
- The issues and risks you face
- Remediation and improvement options – the essential first step is to establish the facts, and evaluate the options with a Network Assessment

The Daisy Network Assessment Services comprise a suite of four discrete components; Network Audit, Network Baseline, Network Healthcheck, and Firewall Healthcheck.

Our consulting engagements are tailored to incorporate any combination of these components as required.

Whether You Are:

- Looking to deploy a converged voice & data network
- Planning or changing a virtualised server environment
- Evaluating 10gb Ethernet options
- Experiencing performance issues
- Planning a network refresh or upgrade

Daisy Network Assessment Services

Network Audit

- Device discovery
- Topology and Configuration audit
- Equipment inventory
- Hardware and software EOL status

Network Baseline

- Capacity assessment of current traffic
- Traffic hotspot identification
- Impact analysis of network configuration changes
- Network performance and utilisation

Network Healthcheck

- Network topology and configuration review versus best practice standards
- Review of network issues contributing to application performance issues

Firewall Healthcheck

- Hardware & Software Version checks
- Firewall Rule Review
- Review for Configuration Best Practice
- Review Security enhancements

Network Audit

Gaining a detailed understanding of your network infrastructure, the software versions it is running, and how it is connected, is key to day to day support and is an essential pre-requisite for planning any network changes or investment.

How the Service Works

Daisy consultants use a structured methodology and utilise automated and manual discovery tools to conduct the engagement in a consistent and thorough way.

Once the audit scope is agreed, Daisy will conduct a structured workshop with key stakeholders, review existing network documentation, including LAN, WAN and structured cabling, and conduct physical inspections of network equipment at sites in scope.

Our consultants will use a combination of Discovery Tools, Network Analysers and Command Line Tools as appropriate to discover all network devices with an IP address, and to retrieve all available inventory data.

We will review the network inventory, topology, IP addressing scheme, and naming conventions against best practice to identify risks, including issues such as known security vulnerability exposure, and vendor end-of-life support withdrawal. Our consultants will rate the issues in their findings report, and propose appropriate remediation options.

Daisy Network Assessment Services

Discover

- Pre-Audit workshop
- Review existing documentation
- Establish device access methods
- Physical inspection
- Network device discovery
- Interconnectivity mapping
- Configuration collection

Assess

- Information analysis
- Hardware and software EOL status
- Findings: issue and risk identification
- Review
- Produce network inventory documentation
- Finalise audit report – findings and recommendations
- Present/review audit report with key stakeholders

Review

- Produce network inventory documentation
- Finalise audit report- findings and recommendations
- Present/review audit report with key stakeholders

How You Benefit

- Document your network assets, providing a detailed inventory and topology baseline from which to assess and develop your network
- Populate your CMDB with an accurate inventory to assist with on-going support
- Improve investment planning through identification of equipment at risk, e.g. as a result of vendor EOL withdrawal of support
- Identify any known security vulnerabilities
- Meet compliance and regulatory obligations through accurate inventory records and an associated risk register
- Gain an independent view from an expert team with a proven methodology, and analysis tool set
- Augment your own team, ensuring focus on urgent projects and support activities

Deliverables

Network Audit report including details of the network topology and IP addressing, providing information by device, location and site (as agreed in the original audit scope):

- LAN / WAN Network diagrams, showing vlans, device IP addresses, hostnames, models, interfaces, and logical connections
- Other network diagrams (Remote access, IP Telephony, Security, Internet, QoS etc)
- Network inventory, showing network device hostname, IP address, make, model, description, serial number, software version, location, critical uplinks, critical downlinks, and End of Life date
- IP addressing scheme
- Naming convention
- Vendor End Of Life Assessment (R/A/G)
- Audit findings, conclusions and recommendations

Presentation:

To the sponsor and key stakeholders on the findings of the audit, risks, priorities, options and next steps.

To find out more about Daisy consultancy services speak to one of our specialists today:

☎ **0800 040 88 88**

✉ sales@daisygroup.com

we are daisy.

www.daisygroup.com