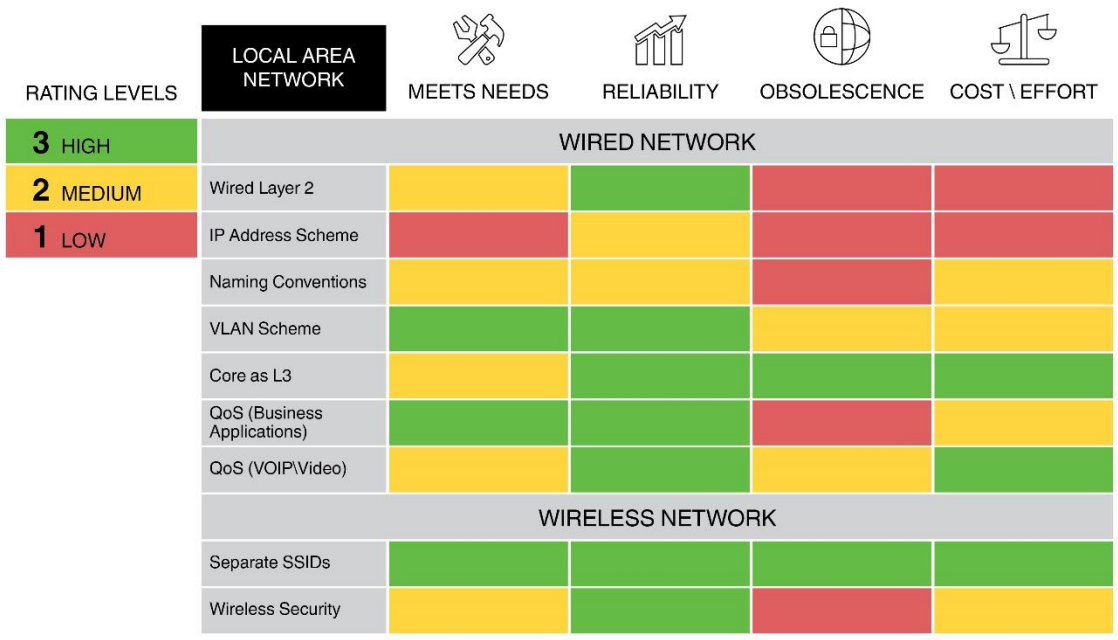
VALUE SCORECARD

NETWORK



ITEM	CURRENT RATING	PREVIOUS RATING
LAN	2.8	N\A

CRITICAL (1 - 2.5)

Serious deficiencies have been identified that require attention within the next year

MODERATE (2.6 - 3.5)

Deficiencies discovered that require attention within the next 2 years

PASS (3.6 -5.0)

No deficiencies discovered

LOCAL AREA NETWORK (LAN)

WIRED NETWORK

CRITERIA		ASSESSMENT
MEETS NEEDS Businesses technology requirements are met		The wired layer 2 and VLAN network infrastructure has a robust VLAN structure in place. The REPNET VLAN is 600 as 'root' of the VLAN scheme. The internal network infrastructure has a further VLAN break-down to business functions and services. Vandelay is applying QoS/Type of Service markings for latency sensitive applications such as VoIP inside its network infrastructure. Maintaining this practice is important since the amount of data competing for bandwidth will only increase, requiring protection of latency sensitive apps.
RELIABILITY Component provides stability and reliability		Overall the network is sound, however there are a number of single point of failure to be noted. Several key components of this network are provisioned as a single device, including the main ('core') network switches (Core switch 5406). . Improper documentation and not using best (ITIL) practices in documentation, updates and use of structured methods, leads to long mean time to repair, unnecessary down-time, loss of credibility and end-user confidence.
OBSOLESCENCE Component is up to date and fully supported		Over the years no formal network architecture has been developed - changes to the infrastructure have been dealt with by point solutions, creating a dispersed and 'island-based' landscape of tools, technology and a multitude of vendors.
COST/EFFORT Includes direct costs (HW/SW) and		As much as the VLAN had a reasonable documentation in place, the actual layer 2 network topology was very poorly documented.

WIRELESS NETWORK

CRITERIA		ASSESSMENT
MEETS NEEDS Businesses technology requirements are met		The wireless network meets the business requirements at this time
RELIABILITY Component provides stability and reliability		The wireless network appears to be stable with minimal downtime
OBSOLESCENCE Component is up to date and fully supported		The wireless services inside the main building is separated with a secure SSID, however the public SSID is unsecure. We noticed several security flaws when using the unsecured SSID
COST/EFFORT Includes direct costs (HW/SW) and indirect costs downtime/operations)		Reasonable effort to maintain with minimal costs for hardware and software

RECOMMENDATIONS

- A Visio diagram should be considered a first step towards documentation, which will have to include logical diagram sections, separating business services by means of color schemes and functions. Properly document the layer 2 and 3 network topologies of all main locations
- Use of industry standard tools, allowing to export, edit and maintain documents rather than using a simple drawing tool and PDF
- Investigate the use of Solarwinds' Network Topology Mapper that allows for real-time and up-to-date network topology maps
- In the context of QoS, performance monitoring and capacity planning, it is essential to utilize and/or implement performance and capacity monitoring solutions.
- These dashboard-type solutions with real-time data give immediate insight into the current state of an infrastructure and allow to act preventively rather than in a reactive mode.
- These monitoring solutions enable the organizations IT to plan ahead of any change, evaluate application load, data storage patterns and protect existing end-user performance SLA.
- We also recommend Vandelay further investigate:
  - How to extend its current monitor platform with performance and capacity planning modules
  - Request SoftChoice to add performance, throughput and bandwidth statistics to their Monthly Vitals Report
  - investigate the SkyDrive/OneNote traffic that is current uploading data into the Cloud
  - Ensure that a fair use policy is in place and have he reflected in the policy rules of the Regions Internet facing gateways/firewalls.
- We would like to recommend the concept that despite the organization having public IP addresses
  - ISIT has the choice to simply not operate like the public Internet and bring back control, predictability, performance and consistency to the IT teams that service the remainder of IT and the entire user community.