SOFTWARE SCORECARD

OVERALL RATING

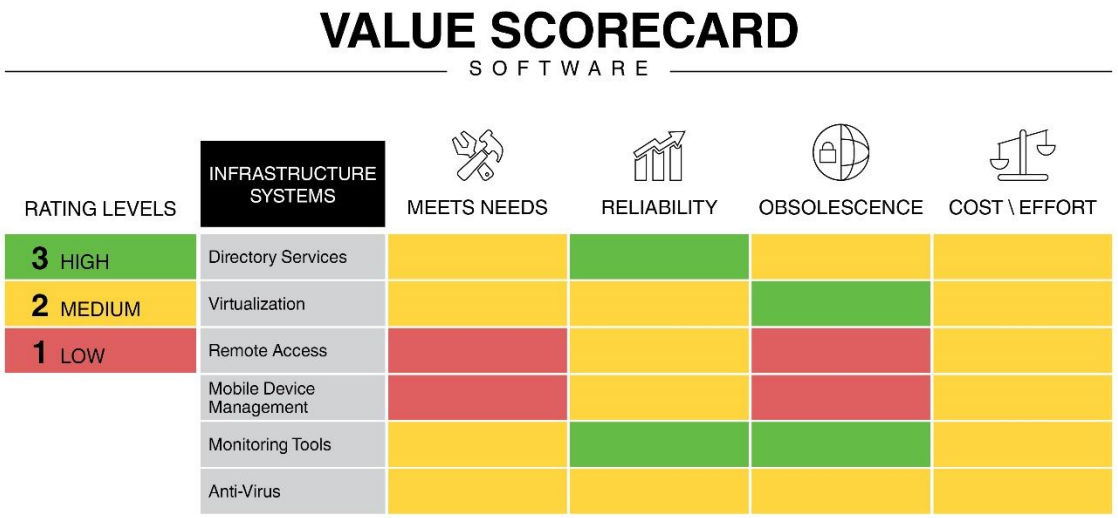
Overall Health Check Rating is based on the rolled-up score of all areas defined within Software: IT Infrastructure Systems.

IT Infrastructure Health Check: Software

May 16th, 2017

Last Year	Infrastructure Systems – Business Systems	Health Check Rating
N/A		3.1

Infrastructure Systems



Item	Current Rating	Previous Rating
Infrastructure Systems	3.1	N/A

Synopsis

The configuration and management of Directory Services (Microsoft Active Directory) is sufficient and adheres to best practices.

The current move to a virtualized infrastructure (servers) is sound but needs to be formally documented.

There is no formal Remote Access policy in place, however there are islands of disparate systems in place to support this service. ITS has recognized this as an issue, and a plan is being developed to implement a formal strategy.

Mobile Device Management (MDM) is available (informally) via Blackberry Enterprise Server (BES). However the Region is planning to adopt a formal strategy in this area (e.g. BYOD, COPE, etc.).

Solarwinds was purchased but resource limitations has prevented the Region from taking full advantage of this product.

Anti-virus is present on all servers and workstations, but steps need to be taken to improve compliance management.

Please refer to the Infrastructure Systems section for the complete review and recommendations

FINDINGS AND RECOMMENDATIONS

SOFTWARE

INFRASTRUCTURE SYSTEMS

The core infrastructure systems reviewed included: Active Directory Services, Server Virtualization Infrastructure, Remote Access, Antivirus, Network Monitoring Tools, and Mobile Device Management.

Directory Services (Active Directory) – There were no major issues or concerns.

Virtualization (Servers) – VMware is the virtualization platform in use at the Region. The infrastructure and consolidation strategy is sound, however the plan has not been formally documented. Planned VMWare clusters: 10 nodes at primary, 5 nodes at DR, 4 nodes at Backup sites.

Remote Access – There are no formal policies in place for remote access which has resulted in several solutions scattered throughout the Regions. There is currently a plan for formalized this service.

Antivirus – Currently using Kaspersky for the servers and Windows Defender on desktops. There appears to be some issues keeping all of the servers up to date.

Network Monitoring Tools – Solarwinds has been implemented for various monitoring activities. There are several modules yet to be activated and the solution has not been fully implemented at this time.

Mobile Device Management – Currently there are Blackberry's being managed (ad-hoc) with a Blackberry Enterprise Server (BES). However, there are no formal policies in place for mobile device management. A Bring Your Own Device (BYOD) is being considered.

Recommendations

- VMware Option: The region could consider putting NVMe into the vSAN cluster - using that single environment for everything rather than pay the Compellent tax on the existing hardware.
  - However the current plan is in fact acceptable and needs to be documented
- The Region needs to invest in an [8]Enterprise Mobility Strategy
  - This step would precede the procurement of the EMM solution
- Remote Access – the Region needs to standardize on a RA solution and eliminate the "islands" of technology that currently exist.
- Antivirus – Servers need to be kept up to date

[8] The biggest mistake organizations make is trying to select an MDM/EMM solution prior to aligning a proper mobility strategy with the business needs. You should have a cross-functional team between the business units and ITS to develop a true mobility strategy.