Baseline Assessment for: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |
| --- |
| **Hardware** |

**Servers:**

|  |  |  |
| --- | --- | --- |
|  | **Not Applicable** | There are no servers. |
|  | **At Risk** | Some servers are past EOL or have warranty that has expired. |
|  | **Needs Attention** | Some servers are approaching EOL or warranty expiration. |
|  | **Satisfactory** | Servers are not approaching EOL or warranty expiration. |

**Workstations:**

|  |  |  |
| --- | --- | --- |
|  | **Not Applicable** | There are no workstations |
|  | **At Risk** | Some workstations are past EOL or have warranty that has expired. |
|  | **Needs Attention** | Some workstations are approaching EOL or warranty expiration. |
|  | **Satisfactory** | Workstations are not approaching EOL or warranty expiration. |

**Operating Systems:**

|  |  |  |
| --- | --- | --- |
|  | **At Risk** | Some Operating Systems are no longer vendor supported, which creates a security risk to the company and places the company out of major industry best practices and compliances. |
|  | **Satisfactory** | All Operating Systems are current and vendor supported. |

**UTM Internet Security Appliance:**

|  |  |  |
| --- | --- | --- |
|  | **At Risk** | Current device is a router only and lacks monitoring and up to date security features. |
|  | **Needs Attention** | Firewall is managed and up to date, but nearing the end of its lifespan. |
|  | **Needs Attention** | Current firewall is not configured to block unwanted content.  |
|  | **Satisfactory** | Supportable UTM Firewall is included and managed. |

**Switches:**

|  |  |  |
| --- | --- | --- |
|  | **At Risk** | Switches are beyond end of life as per company. Firmware updates and security patches will not be made available even if a vulnerability is discovered. |
|  | **At Risk** | Switches are over 5 years old and not cloud managed/monitored. This will have performance implications and increases potential for failure and increased downtime. |
|  | **Needs Attention** | Switches are managed and VLANs are deployed, but cloud visibility is not available, which may impede monitoring and troubleshooting. |
|  | **Satisfactory** | Client has deployed Next Generation cloud managed switches and refreshing them on a schedule as part of regular lifecycle management. |

**WiFI:**

|  |  |  |
| --- | --- | --- |
|  | **Not Applicable** | WiFi does not exist and the organization has no business case to introduce it into the environment. |
|  | **At Risk** | Wireless hardware is beyond end of life. Firmware updates and security patches will not be made available even if a vulnerability is discovered. |
|  | **At Risk** | Wireless is ad-hoc and lacks visibility and management. |
|  | **Satisfactory** | Wireless is managed, separated into VLANs, and allows for guest access separate from corporate data networks. |

**Power Management:**

|  |  |  |
| --- | --- | --- |
|  | **At Risk** | Existing UPS is an EOL and/or does not have enough capacity to support the environment. |
|  | **Needs Attention** | Battery backup is attached to server – however configuration has not been tested. |
|  | **Satisfactory** | Mission Critical equipment is protected by a UPS. |

|  |
| --- |
| **Continuity of Operations** |

**Backup & Disaster Recovery:**

|  |  |  |
| --- | --- | --- |
|  | **At Risk** | Backups are not currently running. |
|  | **At Risk** | Backups require human intervention to run or change media. |
|  | **Needs Attention** | Backup is being performed to Google Drive/Dropbox or other cloud service. |
|  | **Satisfactory** | Onsite BDR appliance caches backups while they replicate to a geo-redundant cloud infrastructure. Solution is separate from the corporate network and resistant to malware/encryption. |
|  | **Satisfactory** | Direct to Cloud backups offer geo-redundancy and both bare metal and file level restore. Solution is separate from the corporate network and resistant to malware/encryption. |

**Backup of Cloud Services:**

|  |  |  |
| --- | --- | --- |
|  | **At Risk** | Microsoft and Google both recommend a third party backup of their cloud services. No such backup has been implemented. |
|  | **Acceptable Risk** | Client understands the risk and is willing to accept the loss of all data stored in third party cloud environments. |
|  | **Satisfactory** | Cloud Backups have been deployed. Monitoring and test restores are part of the Client’s service plan. |

**Business Continuity Plan:**

|  |  |  |
| --- | --- | --- |
|  | **Not Applicable** | Unknown – more information is required. |
|  | **At Risk** | The organization relies on vendors to know what to do when disaster strikes and guide them through the reactionary steps. |
|  | **Needs Attention** | Basic continuity planning exists but is not tested or reviewed regularly. |
|  | **Satisfactory** | The organization has several continuity plans for different potential disaster scenarios. These plans are reviewed annually and updated as necessary. Tabletop exercises are performed at an acceptable time period. |

**Endpoint Security Software:**

|  |  |  |
| --- | --- | --- |
|  | **At Risk** | Anti-virus is installed manually with some machines unprotected or out of date. |
|  | **Needs Attention** | Quality anti-virus is installed and centrally managed. |
|  | **Needs Attention** | Anti-virus is managed internally using a server based console and all endpoints are up to date. |
|  | **Satisfactory** | Traditional Anti-virus was replaced with or is supplemented by Next Gen Endpoint Protection with Endpoint Detection or Response. |

**Hosted Email:**

|  |  |  |
| --- | --- | --- |
|  | **At Risk** | Office uses consumer grade email with minimal security features. |
|  | **Needs Attention** | Email is hosted with Microsoft 365 but security standards are not aligned with best practices. |
|  | **Needs Attention** | Google Apps for Business is in place. We recommend M365. |
|  | **Satisfactory** | Email is outsourced to a 3rd party Hosted Exchange provider or to M365. |

**Email Protection / Filtering:**

|  |  |  |
| --- | --- | --- |
|  | **At Risk** | There is no email anti-spam and/or virus filter in use. The email client provides filtering. |
|  | **Need Attention** | Minimal email filtering is provided by Google Apps but may be insufficient. |
|  | **Needs Attention** | Minimal email filtering is provided by M365 but may be insufficient. |
|  | **Needs Attention** | There is a 3rd party anti-spam and virus filter that is integrated with the hosted Exchange provider. |
|  | **Satisfactory** | Advanced Central Email program is deployed and protecting the email environment. |

**Email Archiving:**

|  |  |  |
| --- | --- | --- |
|  | **Not Applicable** | Client has sensitive data and/or reporting requirements and Email Archiving is not in place. |
|  | **Acceptable Risk** | Email archiving is not in place and the Client accepts the risk of lost or incomplete data searches in the event of a request (ie. FOIA) |
|  | **Satisfactory** | Email archiving is in place to protect sensitive data from loss and/or simplify reporting in the event of a data request (ie. FOIA) |
|  | **Satisfactory** | There is no sensitive information in email. Email is deleted regularly to limit exposure in event of a breach. |

**LoB Application Support:**

|  |  |  |
| --- | --- | --- |
|  | **At Risk** | Client is dependent on out of date software that is not under vendor support. This may lead to stability issues, downtime, and/or security breaches. |
|  | **Satisfactory** | Client’s Line of Business Applications are modern and under vendor support. These applications are included as part of Lifecycle Management planning. |

**Redundant Internet:**

|  |  |  |
| --- | --- | --- |
|  | **Acceptable Risk** | Client is aware that redundant solutions exist, but has identified minimal downtime as an acceptable risk that has minimal impact on the business. |
|  | **Satisfactory** | Client is running 2 ISP circuits in tandem. |
|  | **Satisfactory** | Client has implemented Verizon 4G Wireless **Backup.** |

**Infrastructure Capacity & Scalability:**

|  |  |  |
| --- | --- | --- |
|  | **Not Applicable** | The organization is not planning for expansion at this time. |
|  | **At Risk** | Local resources are at capacity. |
|  | **Needs Attention** | Local resources are limited making scaling the business expensive or difficult. |
|  | **Satisfactory** | The organization’s decision to move to the cloud means that capacity and scalability are flexible and cost effective. The organization can scale as it grows without undue expense or delays. |

**Storage:**

|  |  |  |
| --- | --- | --- |
|  | **At Risk** | Primary data storage is less than 20% free. Low free space can cause issues with back and maintenance tasks. It will impede the company’s ability to scale the business. |
|  | **Needs Attention** | Primary data storage is less that 30% free. Low free space can cause issues with back and maintenance tasks. It will impede the company’s ability to scale the business. |
|  | **Acceptable Risk** | There is no shared storage OR files reside on local workstations. |
|  | **Satisfactory** | Primary data storage is located onsite and offers sufficient room for expansion/growth. |
|  | **Satisfactory** | Primary data storage is in the cloud and scaleable to meet business needs. |

**Remote Access:**

|  |  |  |
| --- | --- | --- |
|  | **Unknown** | More information needed |
|  | **Not Applicable** | Not Applicable |
|  | **At Risk** | VPN Access is required to work remotely. Unmanaged personal devices are being used for remote access. |
|  | **Needs Attention** | VPN Access is required to work remotely. Company equipment is furnished for remote access |
|  | **Satisfactory** | Organization’s infrastructure is built for mobility first/secure remote access by hosting all critical components in the cloud. |

|  |
| --- |
| **Strategic** |

**Asset Inventory:**

|  |  |  |
| --- | --- | --- |
|  | **At Risk** | Asset Inventory is not being performed. |
|  | **Needs Attention** | Asset Inventory is manual for Chromebooks and tablets. |
|  | **Needs Attention** | Asset Inventory is manual and time consuming. |
|  | **Satisfactory** | Asset Inventory is largely automated and included in the service agreement. |

**Network Documentation:**

|  |  |  |
| --- | --- | --- |
|  | **At Risk** | Network documentation is severely lacking which makes the environment difficult to support. |
|  | **Needs Attention** | Because all service hours are billable, network documentation lacks details. |
|  | **Needs Attention** | Network documentation is performed by the MSP but onsite IT does not properly document changes, resulting in a decline in the accuracy of documentation over time. |
|  | **Needs Attention** | Network documentation is incomplete and needs attention. |
|  | **Satisfactory** | Network documentation is performance by the MSP and available upon request. |
|  | **Satisfactory** | Network documentation is performance by the MSP and shared with the company as necessary. |

**Controlled Access/Least Privilege Policy:**

|  |  |  |
| --- | --- | --- |
|  | **Unknown** | Unknown – more information required. |
|  | **At Risk** | The company has no policy in place to limit access rights for users to the bare minimum permissions they need to perform their work. |
|  | **Satisfactory** | The company has a defined policy in place to limit access rights for users to the bare minimum permissions they need to perform their work. |

**Directory Services:**

|  |  |  |
| --- | --- | --- |
|  | **At Risk** | No central source of authentication is in use. This creates unnecessary risk/exposure caused by lack of accountability and an inability to deploy adequate security policies. |
|  | **Needs Attention** | Users, groups, and permissions are managed in Azure (free), which limit group policy capabilities. |
|  | **Satisfactory** | Users, groups, and permissions are authenticated against a robust cloud based authentication system. |
|  | **Satisfactory** | Users, groups, and permissions are authenticated against an onsite Domain Controller. |

**Dark Web Monitoring:**

|  |  |  |
| --- | --- | --- |
|  | **At Risk** | No Dark Web monitoring is in place. |
|  | **Satisfactory** | The Dark Web is being monitored for employee credentials and a process is in place to provide additional training if/when credentials are breached. |

**IT Support Services:**

|  |  |  |
| --- | --- | --- |
|  | **At Risk** | All IT Support is reactive and billable per hour. Budgeting IT support costs is impossible. |
|  | **Needs Attention** | IT Support Agreement includes unlimited remote support, but onsite support is billable and therefore difficult to budget. |
|  | **Needs Attention** | IT Support Agreement includes basic automated tasks, but human intervention when required is billable and therefore difficult to budget. |
|  | **Satisfactory** | IT Support Agreement includes unlimited remote support and onsite support. Moves/Adds/Changes and Projects are billable outside of the agreement. |

**Media Disposal Policy & Procedure:**

|  |  |  |
| --- | --- | --- |
|  | **At Risk** | No secure media disposal P&P is in place. |
|  | **Needs Attention** | The current media disposal P&P is ineffective and leaves significant risk of data exposure/breach to the organization. |
|  | **Satisfactory** | The current media disposal P&P is in place and followed every time hardware is procured and retired from use in the organization. |

**Patch Management Policy:**

|  |  |  |
| --- | --- | --- |
|  | **At Risk** | No defined process exists for deploying Operating System and Application updates on a regular basis. These patches are installed manually and there is no method or process for checking the status. |
|  | **Acceptable Risk** | Some devices cannot be patched due to vendor requirements. Additional steps are being taken to add additional protections but full remediation is impossible. |
|  | **Satisfactory** | A defined process exists for deploying Operating System and Application updates on a regular basis. These patches are audited for successful deployment and remediated if/when failures occur. |

**Technology Budgeting:**

|  |  |  |
| --- | --- | --- |
|  | **At Risk** | Technology budgeting is not being performed regularly, making lifecycle management a difficult or impossible task. |
|  | **Needs Attention** | Technology budgeting is a work in progress but a plan out line is in place. |
|  | **Satisfactory** | The organization has a formal budget in place for all IT products and services. |

**Virtual Networks (VLANs):**

|  |  |  |
| --- | --- | --- |
|  | **At Risk** | The network does not have VLANs deployed which increases the threat from lateral movement of hackers through the network. |
|  | **Needs Attention** | A minimal number of VLANs have been deployed with access rules between them to provide an additional security layer but further segmentation is recommended to achieve best practices compliance. |
|  | **Satisfactory** | A reasonable number of VLANS have been deployed with access rules between them to provide an additional security layer and aid in best practices compliance. |

**vCIO Consulting Services:**

|  |  |  |
| --- | --- | --- |
|  | **At Risk** | Client does not have an engagement for vCIO services. Necessary tasks like Strategic Technology Planning, Budgeting and Technology Alignment are not being performed regularly. |
|  | **Needs Attention** | vCIO Services are readily available under the client’s service agreement but not being fully utilized. |
|  | **Satisfactory** | vCIO Services are included in the service offering and Strategic Business Review meetings are scheduled annually. |
|  | **Satisfactory** | vCIO Services are included in the service offering and Strategic Business Review meetings are scheduled semiannually. |
|  | **Satisfactory** | vCIO Services are included in the service offering and Strategic Business Review meetings are scheduled quarterly. |