Prepared for: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_

**LCI Default Assessment**

*This is the default assessment template shared by Lifecycle Insights. It is aimed at assessing risk in the following categories: Hardware, Business Applications/Software, Security, Continuity, Policy & Procedure, and Regulatory Compliance.*

**Hardware**

Review different components related to client's infrastructure.

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

| **Power Management** |
| --- |
|  | **At Risk**  | Existing UPS is at 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.  |

| **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.  |

| **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.  |

| **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 than 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 in the cloud and scale-able to meet business needs.  |
|  | **Satisfactory**  | Primary data storage is located onsite and offers sufficient room for expansion/growth.  |

| **Spare Device Inventory** |
| --- |
|  | **At Risk**  | The company does not keep spare equipment on hand.  |
|  | **Needs Attention**  | The company keeps only minimal spare equipment.  |
|  | **Acceptable Risk**  | The company keeps only minimal spare equipment.  |
|  | **Satisfactory**  | The company maintains at least 5% spare equipment.  |

| **Switching** |
| --- |
|  | **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.  |
|  | **At Risk**  | Switches are beyond end of life as per Cisco. Firmware updates and security patches will not be made available even if a vulnerability is discovered.  |
|  | **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.  |

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

| **WiFi** |
| --- |
|  | **Not Applicable**  | WiFi does not exist and the organization has no business case to introduce it into the environment.  |
|  | **At Risk**  | Wireless is ad-hoc and lacks visibility and management.  |
|  | **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.  |
|  | **Satisfactory**  | Wireless is managed, separated into VLANs, and allows for guest access separate from corporate data networks.  |

**Business Applications / Software**

Software Applications for Operating and Protecting the Business

| **Hosted Email** |
| --- |
|  | **At Risk**  | Office uses consumer grade email with minimal security features.  |
|  | **Needs Attention**  | Google Apps for Business in in place. We recommend Office365.  |
|  | **Needs Attention**  | Email is hosted with Office 365 but security standards are not aligned with best practices.  |
|  | **Satisfactory**  | Email is outsourced to a 3rd party Hosted Exchange provider or to Office 365  |

| **Email Encryption** |
| --- |
|  | **Not Applicable**  | Users do not send sensitive information by email.  |
|  | **Unknown**  | Unknown - more information is required.  |
|  | **At Risk**  | Sensitive information is being sent by email without encryption.  |
|  | **Satisfactory**  | Users who send sensitive information via email have access to encrypted email.  |

| **Operating System** |
| --- |
|  | **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.  |

| **Software License Management** |
| --- |
|  | **At Risk**  | License Management is not being performed. Client may be at risk of an audit from vendors like Microsoft.  |
|  | **Satisfactory**  | License Management is handled by the IT Provider and the client is believed to be in compliance.  |

**Security**

Review critical areas of security in place for the client.

| **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.  |

| **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 will limit group policy capabilities.  |
|  | **Satisfactory**  | User accounts and permissions are authenticated against an onsite Domain Controller.  |
|  | **Satisfactory**  | User accounts and permissions are authenticated against Azure (paid), which offers a robust cloud based authentication system.  |
|  | **Satisfactory**  | User accounts and permissions are authenticated against Jumpcloud, which offers a robust cloud based authentication system.  |

| **Email Protection / Filtering** |
| --- |
|  | **At Risk**  | There is no email anti-spam and/or virus filter in use. The email client provides filtering.  |
|  | **Needs Attention**  | There is a 3rd party anti-spam and virus filter that is integrated with the hosted Exchange provider.  |
|  | **Needs Attention**  | Minimal email filtering is provided by Office 365 but may be insufficient.  |
|  | **Needs Attention**  | Minimal email filtering is provided by Google Apps but may be insufficient.  |
|  | **Satisfactory**  | Sophos Central Email Advanced is deployed and protecting the email environment.  |

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

| **Intrusion Detection & Prevention** |
| --- |
|  | **At Risk**  | IPS/IDS is not supported on current firewall solution.  |
|  | **Satisfactory**  | IPS/IDS is included as part of Firewall as a Service subscription.  |

| **Virtual Networks (VLANs)** |
| --- |
|  | **At Risk**  | The network does not have VLANs deployed which increases the threat from lateral movement of hackers and malware throughout 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.  |

| **Workstation/Server Encryption** |
| --- |
|  | **At Risk**  | Encryption is not in place on workstations and servers.  |
|  | **At Risk**  | Some workstations are consumer grade and lack TPM hardware required for proper encryption.  |
|  | **Acceptable Risk**  | Mobile Workstations are encrypted but desktops and servers are deemed not likely to be lost/stolen. The company understands the risks in the event that a workstation or server were removed from the o  |
|  | **Satisfactory**  | TPM is activated and Bitlocker encryption is monitored on all systems authorized to contain sensitive information.  |

| **Mobile Device Encryption** |
| --- |
|  | **Unknown**  | More information needed  |
|  | **At Risk**  | Mobile device encryption is not enforced or mandated by company policy.  |
|  | **Acceptable Risk**  | Mobile device encryption is not forced, but is required as per company policy.  |
|  | **Satisfactory**  | MDM policy or Office 365 security policy includes forced mobile device encryption.  |

| **Mobile Device Management** |
| --- |
|  | **At Risk**  | MDM is not in use.  |
|  | **Needs Attention**  | Company owned mobile devices are managed, but personal devices are attached to company data which increases risk/exposure.  |
|  | **Satisfactory**  | MDM is in place and company owned devices are managed and patched regularly.  |

| **Multi-Factor Authentication** |
| --- |
|  | **At Risk**  | MFA is not deployed.  |
|  | **Needs Attention**  | MFA is deployed for Office 365, but needs to be added for other critical systems.  |
|  | **Acceptable Risk**  | MFA is not deployed. Customer is aware of the risks and accepts full responsibility for a breach of critical systems.  |
|  | **Satisfactory**  | MFA is deployed on all critical systems including workstations, servers and web applications.  |

| **Password Manager** |
| --- |
|  | **At Risk**  | No password management solution is in use, or users are left to find a solution on their own.  |
|  | **Satisfactory**  | A Password Manager is in use and shared password vaults are shared among restricted groups only as necessary.  |

| **Scan & Fax to Email** |
| --- |
|  | **Unknown**  | Unknown - more information is required.  |
|  | **At Risk**  | Fax and/or scan to email are in use, causing potentially sensitive information to be stored un-encrypted inside mailboxes.  |
|  | **Satisfactory**  | Fax and/or scan to email are not in use.  |
|  | **Satisfactory**  | A Secure Fax service and/or scan to folder are in use, limiting the potential for sensitive information to wind up in email.  |

| **SIEM** |
| --- |
|  | **At Risk**  | SIEM is not deployed.  |
|  | **Acceptable Risk**  | SIEM is not deployed due to cost. Organization is aware that this additional layer of security may stop threats missed by other layers of security, and is willing to accept the risk.  |
|  | **Satisfactory**  | SIEM is deployed and monitored 24/7  |

| **Social Engineering and Phishing** |
| --- |
|  | **At Risk**  | Insufficient social engineering and/or phishing training is being performed.  |
|  | **Acceptable Risk**  | Training is being performed by the organization, but IT is separated from the process. The organization is aware that not including IT in training and its results may limit the ability of IT to fore  |
|  | **Satisfactory**  | Social engineering and phishing training is performed at least quarterly and employees are identified who require further training. A process is in place to provide additional training as needed.  |

| **Synchronized Security** |
| --- |
|  | **At Risk**  | Synchronized Security is not a feature of the Firewall and/or Security software.  |
|  | **Needs Attention**  | All the components are in place, but not configured. Project is recommended.  |
|  | **Acceptable Risk**  | Synchronized Security is either not available or not configured. The client is aware of the risk and assumes liability.  |
|  | **Satisfactory**  | Next Generation Endpoint Protection shares threat information with the UTM Firewall, enabling the two to work together to respond to detected threats immediately and without human interaction.  |

| **Third Party Penetration Testing** |
| --- |
|  | **At Risk**  | Client is in a high compliance industry, yet is not hiring a third party to perform Penetration Testing at regular intervals.  |
|  | **Acceptable Risk**  | Third Party Penetration Testing is cost prohibitive. Client accepts the risk of not having these tests performed.  |
|  | **Satisfactory**  | Third Party Penetration Testing is performed on an interval deemed acceptable based on the client's risk profile. Results are added to remediation planning and addressed based on risk/exposure.  |

| **VPN / Remote Access** |
| --- |
|  | **Not Applicable**  | Not Applicable  |
|  | **Unknown**  | More information needed  |
|  | **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.  |

| **Vendor Risk Management** |
| --- |
|  | **Unknown**  | Unknown - more information is required.  |
|  | **At Risk**  | Vendor risk audits are not being performed.  |
|  | **Needs Attention**  | Some vendors are asked to complete risk audits, but the audits are not regularly scheduled and/or required for all vendors.  |
|  | **Acceptable Risk**  | No vendors have access to sensitive data, or the risk has been deemed minimal. Vendor risk audits are not being performed and the company accepts the risk that this may introduce.  |
|  | **Satisfactory**  | All vendors are required to complete an audit annually to ensure reasonable security based on their level of access and sensitivity of their access to corporate data. Policies are in place to address  |
|  | **Satisfactory**  | Vendors with access to sensitive data are required to complete an audit annually to ensure reasonable security. Policies are in place to address vendors who score poorly on an audit.  |

| **Website Management** |
| --- |
|  | **Unknown**  | Unknown - more information is required.  |
|  | **At Risk**  | No resource is currently maintaining the company website. Website patches and security fixes may need to be applied.  |
|  | **At Risk**  | The organization has an outsourced resource for managing the company website. That resource does not collaborate with the MSP for changes, which could result in downtime for the organization.  |
|  | **Satisfactory**  | The organization has an outsourced resource for managing the company website. That resource is documented and collaborates with the MSP for any DNS changes.  |

**Continuity**

Business Continuity and BDR

| **Backup & Disaster Recovery** |
| --- |
|  | **At Risk**  | Backups require human intervention to run or change media.  |
|  | **At Risk**  | Backups are not currently running.  |
|  | **Needs Attention**  | Backup is being performed to Google Drive/Dropbox or other cloud service.  |
|  | **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.  |
|  | **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.  |

| **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.  |

| **Cloud File Server** |
| --- |
|  | **Not Applicable**  | Not Applicable.  |
|  | **Unknown**  | More information needed  |
|  | **At Risk**  | Business files are hosted on an internal file server, and files are being accessed by unmanaged computers, putting the entire organization's data at risk.  |
|  | **Needs Attention**  | Business files are hosted on an internal file server, and accessibility from the outside requires either VPN or another form of remote access.  |
|  | **Satisfactory**  | Business files are hosted on geo-redundant cloud infrastructure. Proper security is being applied while desktop and mobile accessibility are readily available for those who require it.  |

| **Email Archiving** |
| --- |
|  | **At Risk**  | 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 (i.e. FOYA)  |
|  | **Satisfactory**  | There is no sensitive information in email. Email is deleted regularly to limit exposure in the event of a breach.  |
|  | **Satisfactory**  | Email Archiving is in place to protect sensitive data from loss and/or simplify reporting in the event of a data request (i.e. FOYA).  |

| **Print Management** |
| --- |
|  | **Unknown**  | More information needed  |
|  | **At Risk**  | Wireless printers are in use. The lack of reliability in wireless printing significantly increases the risk of downtime.  |
|  | **Needs Attention**  | A number of inefficient desktop printers throughout the company make printing difficult to support and more expensive than necessary.  |
|  | **Satisfactory**  | Printing is handled centrally by high volume print/copy devices with desktop printers only deployed for sensitive print jobs.  |

| **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 has implemented Verizon 4G Wireless Backup  |
|  | **Satisfactory**  | Client is running 2 ISP circuits in tandem.  |

| **Internet Service** |
| --- |
|  | **Needs Attention**  | ISP is unreliable and/or circuit speed is inadequate for the operations of the business.  |
|  | **Satisfactory**  | ISP is reliable and circuit speed is appropriate for the operations of the business.  |

| **Infrastructure Wiring** |
| --- |
|  | **At Risk**  | Infrastructure wiring is disorganized and lacks labeling, adding downtime in the event of a network issue.  |
|  | **Satisfactory**  | Infrastructure wiring is reasonably clean and well labeled, speeding up the troubleshooting process in the event of a network issue.  |

**Policy & Procedure**

Does the company have the necessary Policies & Procedures in place to provide appropriate protections?

| **Acceptable Use Policy (AUP)** |
| --- |
|  | **Unknown**  | Unknown - more information is required.  |
|  | **At Risk**  | No AUP exists. Client has little recourse if technology is misused.  |
|  | **Satisfactory**  | AUP is in place and regularly updated to keep up with changing threat landscape. The AUP and updates to it are shared with IT Service Provider and signed by all staff members.  |
|  | **Satisfactory**  | AUP is in place and signed by all staff members.  |

| **Access Logging** |
| --- |
|  | **Unknown**  | Unknown - more information is required.  |
|  | **At Risk**  | Client is not logging access to sensitive areas (server rooms, restricted printers, etc).  |
|  | **Satisfactory**  | Sensitive areas are monitored by cameras and access is logged.  |

| **Controlled Access / Least Privilege Policy** |
| --- |
|  | **Unknown**  | Unknown - more information is 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  |

| **BYOD Policy** |
| --- |
|  | **Unknown**  | Unknown - more information is required.  |
|  | **At Risk**  | Bring your own device policy is not in place. Users can access company data from personal devices like phones and tablets.  |
|  | **Acceptable Risk**  | BYOD policy has been developed, is signed by every employee, updated regularly, and shared with the MSP.  |
|  | **Satisfactory**  | BYOD policy is in use and enforced by Microsoft Intune.  |
|  | **Satisfactory**  | BYOD policy is in use and enforced with third party software.  |

| **Data Encryption Policy** |
| --- |
|  | **Unknown**  | Unknown - more information is required.  |
|  | **At Risk**  | Data Encryption Policy exists but is has not been shared with the Service Provider or is not being monitored.  |
|  | **At Risk**  | No Data Encryption Policy exists.  |
|  | **Satisfactory**  | Client has a documented Data Encryption Policy. It has been shared and is on file with the Service Provider, and has been implemented. Software is being used to monitor results in near real time.  |

| **Electronic Funds Transfer Policy** |
| --- |
|  | **Unknown**  | Unknown - more information is required.  |
|  | **At Risk**  | Client does not have an established EFT Policy  |
|  | **Satisfactory**  | Client has an established EFT Policy, updates it regularly, and reviews it with staff at least annually.  |

| **Lifecycle Management Policy** |
| --- |
|  | **At Risk**  | Lifecycle Management is not being performed regularly, leading to significant technology debt and increased risk for the organization.  |
|  | **Needs Attention**  | A significant portion of IT infrastructure has the same EoL dates due to a lease or large purchase. Client should be aware and planning for this date.  |
|  | **Acceptable Risk**  | A significant portion of IT infrastructure has the same EoL dates due to a lease or large purchase. Client should be aware and planning for this date.  |
|  | **Satisfactory**  | Lifecycle Management is being performed regularly, limiting technology debt and decreasing risk for the organization.  |

| **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.  |

| **Mobile Device Policy** |
| --- |
|  | **Unknown**  | Unknown - more information is required.  |
|  | **At Risk**  | Mobile Device Policy exists but is has not been shared with the Service Provider or is not being monitored.  |
|  | **At Risk**  | No Mobile Device Policy exists.  |
|  | **At Risk**  | Mobile Device Policy exists but does not account for personal devices, leaving the client at risk for exposure.  |
|  | **Satisfactory**  | Client has a documented Mobile Device Policy. It has been shared and is on file with the Service Provider, and has been implemented. It includes policies and safeguards for personal and business own  |

| **Password Policy** |
| --- |
|  | **Not Applicable**  | Password Policy is included in another company policy such as AUP or Employee Manual.  |
|  | **Unknown**  | Unknown - more information is required.  |
|  | **At Risk**  | No Password Policy exists at this time.  |
|  | **At Risk**  | Some users have passwords that are set to never expire.  |
|  | **Satisfactory**  | Password Policy is in place, regularly updated and signed by employees. It is shared with IT Support Vendor.  |
|  | **Satisfactory**  | Password Policy is in place and includes mandatory MFA where available. The Policy is regularly updated, signed by employees and is shared with IT Support Vendor.  |

| **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 of  |
|  | **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 due to vendor requirements. .  |
|  | **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.  |

| **Removable Media Policy** |
| --- |
|  | **Unknown**  | Unknown - more information is required.  |
|  | **At Risk**  | No removable media policy exists. Data is at risk of being exposed via USB drive or other removable media.  |
|  | **Satisfactory**  | Removable Media Policy is in place, signed by all staff members, and enforced with a software solution.  |
|  | **Satisfactory**  | Removable Media Policy is in place and signed by all staff members.  |

| **User Account & Security Permissions Audit Policy** |
| --- |
|  | **At Risk**  | User accounts are not being audited, leaving potential for access from former employees or those with permissions above those required to perform their job function.  |
|  | **Satisfactory**  | Regular Security Audits are being performed to ensure that stale user accounts are removed/deactivated and that users have the least level of privilege to perform their job functions.  |

**Strategic**

Strategic Processes and Initiatives

| **BDR Test Restore** |
| --- |
|  | **At Risk**  | The organization is not performing test restores and relies solely on backup logs to determine viability of backups.  |
|  | **Needs Attention**  | The organization relies on automated test restores and/or screenshot verification, and is not performing manual confirmation of restored data.  |
|  | **Satisfactory**  | The organization has a plan in place for test restores. Test restores are performed on a scheduled basis and successful within acceptable RTO and RPO.  |

| **Business Continuity Plan** |
| --- |
|  | **Unknown**  | 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 acceptabl  |

| **Cyber Liability Insurance** |
| --- |
|  | **Unknown**  | Unknown - more information is required.  |
|  | **At Risk**  | Cyber Liability is an add-on to E&O or other business insurance and has not been vetted by a third party Cyber Liability expert. Loopholes and limitations may exist that would preclude the insurance  |
|  | **At Risk**  | The organization does not currently have Cyber Liability insurance. It is recommended that the organization consult an insurance expert and procure a suitable insurance policy.  |
|  | **Acceptable Risk**  | Client has specific Cyber Liability insurance that NOT been vetted by a third party Cyber Liability Expert for coverage amount and scope. Loopholes may exist that would preclude the insurance carrier  |
|  | **Satisfactory**  | Client has specific Cyber Liability insurance that has been vetted by a third party and deemed appropriate in coverage amount and scope.  |

| **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.  |

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

| **Network Documentation** |
| --- |
|  | **At Risk**  | Network documentation is severely lacking which makes the environment difficult to support.  |
|  | **Needs Attention**  | Network documentation is incomplete and needs attention.  |
|  | **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**  | Because all service hours are billable, network documentation is lacking details.  |
|  | **Satisfactory**  | Network documentation is performed by the MSP and shared with the company as necessary.  |
|  | **Satisfactory**  | Network documentation is performed by the MSP and available upon request.  |

| **Technology Budgeting** |
| --- |
|  | **At Risk**  | Technology Budgeting is not being performed regularly, making lifecycle management a difficult or impossible task to keep up with.  |
|  | **Needs Attention**  | Technology Budgeting is a work in progress, but a plan outline is in place at this time.  |
|  | **Satisfactory**  | The organization has a formal budget in place for all IT products and services.  |

| **Updated Contact Information** |
| --- |
|  | **Not Applicable**  | Due to company size, all key decisions go through the Owner  |
|  | **At Risk**  | The company does not update the MSP when roles transition, making communication difficult when an event occurs.  |
|  | **Needs Attention**  |  Updating Contact Information is a work in progress, but a plan is in place as of this meeting.  |
|  | **Satisfactory**  | The company regularly updates key contact information with the MSP. (Primary contact, Building Access contact, Breach Notification contact, After Hours contact, etc)  |

| **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 quarterly.  |
|  | **Satisfactory**  | vCIO Services are included in the service offering and Strategic Business Review meetings are scheduled semi annually.  |
|  | **Satisfactory**  | vCIO Services are included in the service offering and Strategic Business Review meetings are scheduled annually.  |

**Regulatory Compliance**

Identify and Score Client Compliance Obligations

| **HIPAA Regulatory Compliance**  |
| --- |
|  | **Not Applicable**  | Client does not operate as a Covered Entity or Business Associate.  |
|  | **At Risk**  | Client is a Covered Entity or Business Associate and alignment with the HIPAA rule is insufficient.  |
|  | **Satisfactory**  | Client has a Compliance Process in place and is continually working from a recent SRA and Improvement Plan.  |

| **NIST 800-171 Compliance** |
| --- |
|  | **Not Applicable**  | Client is not obligated to maintain NIST 800-171.  |
|  | **At Risk**  | Client is a Government Contractor and is not in full alignment with NIST 800-171.  |
|  | **Needs Attention**  | Client has performed a full Risk Assessment but has work to do to achieve alignment with NIST 800-171  |
|  | **Satisfactory**  | Client has performed a full Risk Assessment and is continually working to achieve/maintain compliance with NIST 800-171.  |

| **PCI Compliance** |
| --- |
|  | **Not Applicable**  | Client does not handle payment card data.  |
|  | **Unknown**  | Unknown - more information is required.  |
|  | **At Risk**  | Client handles payment card data but has not met the regulatory compliance obligations of PCI.  |
|  | **Needs Attention**  | Client has performed some measures to protect payment card data but is not fully compliant.  |
|  | **Satisfactory**  | Client regularly completes their PCI compliance questionnaire with input from the IT team and is following the compliance recommendations of their processor or PCI Compliance Consultant..  |

| **Business Associate Agreements** |
| --- |
|  | **Unknown**  | Unknown - more information is required.  |
|  | **Not Applicable**  | Client does not operate as a Covered Entity or Business Associate.  |
|  | **At Risk**  | Business Associate Agreements are not in place with all applicable vendors or are outdated.  |
|  | **Satisfactory**  | Business Associate Agreements are in place with applicable vendors and renewed annually.  |