Name	Description	Answer
Security Baseline	Do you roll out a security baseline configuration across servers, laptops, desktops and managed mobile devices?	
Security Training	Do you provide Security Training for All Employees on Annual Basis?	
Phishing Prevention	Have you implemented any of these to protect against phishing messages?	
PowerShell Best Practices	Do you implement PowerShell best practices defined by Microsoft?	
Software End of Life	Do you have any end of life or end of support software in active use?	
Software End of Life Segregated	If you have any end of life or end of support software, is it segregated from the rest of your network?	
Whitelisting/Blacklisting	Do you enforce application whitelisting/blacklisting?	
Deployed Assets	Do you record and track all software and hardware assets deployed across your organization?	
Intune or Similar	Do you run Microsoft Intune or similar patch management system?	
Patching Cadence	How often do you apply patches after they are released?	
Next-generation Antivirus	Do you use a next-generation	

	antivirus (NGAV) product to protect all endpoints across your enterprise?	
Endpoint Detection and Response	Do you use an endpoint detection and response (EDR) tool that includes centralized monitoring and logging of all endpoint activity across your enterprise?	
Endpoint Application Isolation	Do you use endpoint application isolation and containment technology on all endpoints?	
PCI DSS v.3.2	Payment Card Industry Data Security Standard?	
HIPAA	Health Insurance Portability and Accountability Act?	
GDPR	EU General Data Protection Regulation?	
Permissions Management	Do you use Centralized Permissions Management?	
Device Management (MDM/UEM)	What service do you use to manage device endpoints for your network?	
Protective DNS	Prevents access to malware, ransomware, phishing attacks, viruses, malicious sites at the source,	
SIEM/SOC	Do you utilize a Security Information and Event Management system (SIEM) Such as Microsoft Sentinel?	
Vulnerability Management	Do you use a vulnerability management tool?	
Identity Provider	Do you use an IDP (Identity Provider)	
Device Rollout	How do you roll out new	

	devices?	
Security Skills	Do you have a security skills Gap?	
MFA	Do you use Multi-factor authentication to protect all local and remote access, and all user accounts, on all systems including Cloud accounts?	
MFA Remote and RDP	Do you use MFA for your Remote Desktop Protocol, if RDP is used?	
MFA with Azure/Office365	What do you use to enforce MFA?	
Conditional Access and Per-User-Mfa	Do use both Conditional Access and Per-User-Mfa? (not recommended)	
MFA Azure Devices	Do you require MFA when adding devices to Azure AD?	
Conditional Access Benchmarking	If using Conditional Access, do you Benchmark?	
Conditional Access Users not Logged in	If using Conditional Access, do you know what rules apply to users who have yet to log in or who have not logged in for a while?	
Conditional Access Test	If using Conditional Access, do you actively test all your rules on all login types?	
MFA Choices	Do you use one of these for MFA?	
Remember MFA	Do you set the 'Allow users to remember MFA on devices they trust' setting to Disabled?	
PIM/PAM	Do you manage privileged accounts using privileged account management software?	

PIM/PAM	Do you use one of these PIM/PAM Providers?	
Bring Your Own Device	Can users access the network with their own device (Bring Your Own Device)?	
BYOD Enrolled	Do you allow personal devices / BYOD, requiring devices to be full enrolled?	
BYOD Not Enrolled	Do you allow personal devices / BYOD, **NOT** REQUIRING devices to be full enrolled?	
Microsoft Defender Alerts	Do you use Microsoft Defender Alerts?	
Microsoft Sentinel Alerts	Do you use Microsoft Sentinel Alerts?	
Actively Monitor Administrators	Do you actively monitor all administrator access for unusual behavior patterns?	
Non-IT user rights	Do non-IT users have local administration rights on their laptop / desktop?	
Self Password Resets	Do you allow self-service password resets?	
Least Privilege	Do you have a least privilege model or use Zero Trust principles?	
Regular User Azure License	What level of Azure License do you have for Regular users?	
Restrict Guest Invitations	Do you restrict guest invitations to administrators to ensure only authorized accounts have access to cloud resources?	
Guest Invitations	Do you make sure non-admin users cannot invite guests, guests cannot invite guests, and guest invites cannot be sent to	

	any domain?	
Guest Review	If a guest no longer need access, do you remove or disable their guest account?	
Restrict Application Registration	Do you prevent non admin users from registering or consenting to applications that can access organizational data?	
App Registration Audits	If using App Registrations, do you regularly audit and review the App Registration configurations?	
Admin Azure License	What is your Azure security related license for your Admins?	
Finance Azure License	What is your license finance users?	
Restrict Global Admins	How many global administrator accounts (accounts with super user privileges) currently exist on your network?	
Password Reset Notification	Do you enable user notification on password reset? It helps the user to recognize unauthorized password reset activities	
Password Reset Identification	Setting up dual identification for password reset ensures user identity is confirmed via two forms of ID. Do you set the Number of methods required to reset to 2?	
Audit Log Montoring	Do you use audit log montoring?	
Threat Analytics	Do you use Threat Analytics?	
End user audit	How often do you audit your end-users?	
Office365	Every Office 365 subscription comes with Office 365 Defender,	

	are you using it?	
DLP	Data Loss Prevention monitors the activities that users take on sensitive items at rest, sensitive items in transit, or sensitive items in use and take protective actions. This includes controls for Document Sharing, securing your OneDrive and SharePoint files from internal and external threats, and preventing data exfiltration. Are you using it?	
0365 Security	Office 365 reporting includes metrics like as Data Loss Prevention policy matches, Malware detection, Spoof and Spam Detection and many others. Are you using it?	
Microsoft Office Macros	Can users run Microsoft Office Macro enabled documents on their system by default?	
Microsoft 365 Defender	Defender for Business is optimized to meet the needs of small and medium businesses of up to 300 users. Are you using it?	
Defender for Cloud	Defender for Cloud is a solution for cloud security posture management (CSPM) and cloud workload protection (CWP) that finds weak spots across your cloud configuration, helps strengthen the overall security posture of your environment, and can protect workloads across multi-cloud and hybrid environments from evolving threats. Are you using it?	

Microsoft Sentinel	Microsoft Sentinel is an Integrated threat protection with SIEM & XDR, taking in all the information from the Defenders and Senserva and helping you act on it. Are you using it?	
Backup Used	Do you use a backup solution?	
Air-gapped Backup	Are Backups kept locally but separate from your network (offline/air-gapped backup solution) if not in the Cloud?	
Cloud-Syncing	Do you use a Cloud based backup?	
Immutable/Encrypted Backup	Are your backups immutable and encrypted?	
Backup Credentials	Are your backups secured with different access credentials from other administrator credentials?	
MFA for Backup	Do you utilize MFA for both internal and external access to your backups?	
Test Backup Integrity	Can you successfully test your backup integrity, and if so, have your tested in the last 6 months?	
Incident Response plan	Do you have a written incident response plan in the event that Personally Identifiable Information is or may be compromised?	
Business Continuity	Do you have a tested Business Continuity or Disaster Recovery Plan in place that covers cyber event scenarios, such as natural disasters and/or ransomware attacks?	
Network Disruption Recovery	In the case of Network Disruption, what would be your	

	Recovery Time?	
App Registration Permission Review	Do you have a process to review the permissions before they are granted?	
App Registration Creation Review	Do you have a process to review the design before they are created?	
App Registration Owners	Are all App Registrations Owners known and documented?	
App Registration Users	Are all App Registrations Users known and documented?	
App Registration Email Permissions	Can you confirm no registration has permission to edit and/or send emails on behalf of users?	
App Registration Privilege Escalation Permission	Can you confirm no registration has ability to escalate their own permission level?	
App Registration Certificates/Secrets	Can you confirm no App Registration has expired or soon-to-expire Certificates or Secrets?	