| **Step** | **Domain** | **Minimum Acceptable Level** | **Key Topics for Discussion** |
| --- | --- | --- | --- |
|  | Digital Identities | * Directory Services of any kind are used * Unique IDs are used * Permissions are assigned via Groups in the Directory Service * There is an adequate password policy in place * Service and Cloud accounts are gathered, minimized, and under control * Sensitive files are shared in a secure way | * How many people are present in the company? Get overview of employees’ org chart/roles, and how many people are in IT and Security. * How old is the company? Get brief history, acquisitions, etc. * Which DS is used? (AD, which version?) * Get overview of Groups, GPOs, shared accounts, shared mailboxes, federated services, password policy (for AD, request screenshots). * Is every system and device connected to DS and follow password policy, or there are systems which have their own passwords (e.g. Wi-Fi, network devices, etc.)? * What is the process by which Group ownership, permissions and accesses to systems and applications are granted? * Get overview of Cloud services used and how accounts are managed, if SSO is used and how, especially concerning files and documents sharing with third parties. * Is Cloud Sharing such as Box, Dropbox etc. being used? |
|  | Admin Accounts | * Admin accounts are managed under a Directory Service * Admin accounts are unique for each admin * Central ownership of who gets appropriate rights * Process for removing rights as appropriate | * Get overview of how administration is performed, if AD Groups and GPOs are used, if shared accounts and/or shared mailboxes are used for admin accounts * Understand how permissions are granted and removed from users as their work and function changes in the company |
|  | Endpoints / Client Systems | * Client types are reduced as much as possible * Clients use a supported Operative System * Users have restricted access to admin accounts on clients * Disk encryption is applied, especially for mobile systems * Security patches on clients are applied at least monthly * There is a procedure to update software at least quarterly, or after major releases * AV from a reputable vendor is installed, and signatures are updated at least daily * A secure procedure is defined for software updates and new software rollout * A client disposal process is in place * A protection for threats coming from emails is in place * Awareness against phishing is performed * An adequate restriction (by means of technical access control, physical access restriction, or procedural) on allowing access to the Office Network only to authorized devices and people, is in place * Precautions are in place for company devices brought on business trips | * Which clients are used, in terms of variety of systems/operative systems/hardware managed? Is there a client standard? Which one is it? Is a golden image used? * Get overview of client licenses. * What are the standard Anti-virus, client-based firewall/HIPS, URL filtering, and VPN software – if used? * What is the patch rollout schedule on clients, for both security fixes and software updates? Are patches installed securely? Can users override or block patches’ installations? * What kind of hardening is used on clients? Is disk encryption enforced? * Are clients disposed securely after use? Are disks erased? * What is the standard anti-spam protection? * Is awareness against phishing performed on employees? * Understand characteristic and security of Office LAN; is any kind of client authentication used? * Do people work from home? How many? What is the remote setup for home office? Is a VPN used? is split horizon used in home office or VPN connection? Is automatic VPN used? How people access office resources? * How many people use mobile connections? How many people travel and with which frequency? Do they travel to high risk countries? Is there a business trip security awareness training and/or standard in place? * Are office/building facilities shared with other companies? * Do users have access to administrative accounts on their clients? Can they disable security functions or are there mitigations in place for this? |
|  | Servers | * Minimum level of physical restriction are applied to server access * There are some forms of malware mitigation in place on servers, such as an AV from a reputable vendor; signatures are updated at least daily * Software installation and updates must have a secure procedure * Security patches on servers are applied at least quarterly * There are central repositories for rules, security controls and priorities * Some form of hardening is applied for servers which host critical assets | * Get overview of server systems and types (Windows, UNIX, Linux, etc.). * Are servers and other key systems placed in a proper server room? * Is the server room shared with other companies? * What is the frequency and schedule for patches installation on servers? Is there a staged process (e.g. DEV/UAT/PROD) in place for testing patches? Is there a different priority for security patches? Can you rollback them? * What is the malware protection in place for servers? Anti-virus, host-based firewalls?... * Is there some form of vulnerability assessment, hardening and/or compliance program in place? |
|  | Networks | * Secure connectivity between ResMed and target * Secure access from Target staff and stakeholders * Redundant/resilient connections to the Internet are in place * Periodic security controls review for compliance * At least some form of network segmentation and/or filtering segregates critical assets | * Document Internet outbreak. Which kind of connectivity is in place? Are there redundant and resilient network connections? Which kind of failover is in place? Are backup lines or BGP used? Is there MPLS or other private circuits with other offices in place? * Get a list of IP addressing – both public and private usage, as well as network maps. * Are networks segmented in any way (VLANs, subnets, etc.)? How is segmentation used and what does segregate? Is there a segregated management LAN for IT infrastructure? Are critical assets and Tier-1 services segregated from other assets? Is there a segregated voice/video LAN? Is there a DMZ? * How is Office Network secured? Is there any form of NAC? |
|  | Hosting | Minimal controls include:   * contract controls * confirmation of hosting partners security controls * policies for Target hosting and cloud usage * security controls to protect / encrypt co-hosted data | * Describe local and other hosting – data rooms, data centers, etc. * Describe the business applications used – ERP, CRM, etc. Get an overview of the licensing. * Is a web site present? Is a web shop used? How does that interface with the ERP and CRM systems? * Are Cloud services used for sensitive data? What are the protections in place? Is any form of encryption used for hosting of sensitive data? |
|  | Email | * Email use policy in place * User awareness for email security and anti-phishing * Tools and processes for anti-phishing, malware and anti-spam | * Is there any form of IT acceptable use policy which employees sign? Document the policy. * Is awareness or training against phishing attacks performed? * What is the email security tool used? Has this worked well in the past? What is the general awareness level of the employees against social engineering attacks? * Do employees understand the difference between private and corporate use of IT resources? What is the general practice? * Document architecture of email infrastructure and protection measures. Is email hosted internally or externally? Which technology is used? What are the MX, SMTP relay and backbone servers? Are SPF, DKIM and DMARC setup? |
|  | Data Recovery | * Proven data backup / recovery capabilities * Testing of solutions * Viable DR plan | * Describe data backup and DR setup, capabilities and procedures. * Are there documented backup procedures, and a viable DR plan? Are these tested and rehearsed periodically? * Has the business requested precise RTO/RPO for Tier-1 applications? Are the Tier-1 applications identified (e.g. the ERP)? * Are off-site backups performed? |
|  | Boundary Defenses | * Reputable brands and management of Firewalls are in place * Reputable brand of URL filtering/proxies, filtering from threats coming from web browsing, are in place * VPNs are used for B2B communication and remote access of users * Adequate encryption in transit and/or at rest is in place for business applications * Web services are adequately protected | * Which firewalls and proxies are used, and which service license (e.g. URL filtering, IDS/IPS, etc.) are in place? Are NGFW (Layer-7 firewalls) used? * Document the Internet presence (public IP addresses assigned), if web or hosting of other services (FTP, OWA, etc.) is performed from internal networks. * Where is web presence offered from? Is a web shop in place? * Is there a form of protection against Internet attacks and DoS/DDoS? WAF? * Are services offered to employees to work from home (VPN and which kind, Terminal Services, etc.)? * Are there network connections with partners or subsidiaries? Are they using IPsec site-to-site tunnels, or what else? * Are contractors and/or other externals getting connection into the internal networks? In which way? |
|  | Inventory | * Full asset inventory * Network diagrams | * Is there some form of asset inventory? Is it done for laptops, servers, software, mobile devices? * Are there maintained network diagrams and/or IP databases? * Is there an asset management system, and is reconciliation performed between the asset management and the inventory system? |
|  | Operational Security | * A hiring processes is in place * Training is delivered to new employees * Log management and review is in place * Monitoring processes and capabilities are in place * Multi-Factor authentication is used for key systems and remote access * Periodic vulnerability assessments and pen tests are conducted * Process for mitigating critical findings is in place * Encryption of mobile systems and sensitive data is in place * Tested and periodically updated incident response plan is in place | * Is there a hiring process? Are there pre-hiring screening procedures performed for sensitive personnel (e.g. IT admins)? * Are trainings for ResMed policies and standards assigned? Is the training platform and access to the ticketing system delivered? * Are periodic reviews of access rights, separation of duties, and logs performed? Document evidence of this activity has been performed. * Are syslog and audit logs configured and secured for at least Tier-1 applications and critical IT infrastructure? Is there a tamper-proof logging system in place? * Is some form of multiple factors authentication for remote access used? Is it used for all kind of remote access? Is it used for accessing critical systems? * Are periodic reviews, penetration testing, tabletop or red/blue team exercises performed? Are they done through an external firm? Document the most recent assessments. * Are there exemption and mitigation processes for security findings in place? Is there an emergency plan for critical security events? * Is there some kind of central log collection and/or dashboard from which to assess holistically the security posture? * Are there a vulnerability management and a patch management process? * Is there a process for periodic testing and hardening? * Is there an incident response plan? Is this rehearsed? Is it periodically updated? Document the last exercise. * Does the organization have a Privacy officer? * Does the organization maintain certifications such as ISO 27000 series, ISO 9001, etc.? |
|  | Physical | * Physical Security plan * Access control systems * Critical/High Impact IT infrastructure is physically segregated * Physical access is logged/monitored | * Is the server room shared with other entities? Who can access the server room? What are the access controls for it? * Are key systems hosted in different physical servers? Are they replicated? Is there a geographically diverse, replicated copy of the system? * What are the security protections for the data room/data center? Are accesses logged and monitored? * Are backups also protected? |
|  | Wireless | * Wireless segregated from Critical/High Impact IT infrastructure * Corporate and guest networks are separated * Wi-Fi monitoring and access control are in place * Site perimeter is monitored | * What are the wireless capabilities offered? Is there a corporate and guest Wi-Fi? * How is corporate Wi-Fi provided? What is the architecture of the access points? Which technology, security and encryption are used? If present, how is the guest Wi-Fi managed? * Is an MDM used? Are NAC controls in place? * Are periodic wireless surveys performed? Are rogue AP detected? Is there a policy to shut them down? * Is the Wi-Fi range controlled? Can wireless networks be reached outside of the perimeter of the organization? |