Gap Analysis Report

SLB + Solubon Ltd.

Prepared by: Ashfaq Khan

Date: 7/16/2025

I. OVERVIEW

The company's IT foundation has several solid elements in place, including WPA3-secured Wi-Fi, a functioning patch panel with switches, Microsoft 365 Business Premium with Defender v2, and Barracuda for general backup. However, there are key areas that require immediate attention as Solubon merges into SLB. These include finalizing administrator transitions, implementing a secure VPN for all endpoints (including mobile), standardizing hardware and antivirus across devices, and optimizing productivity within the Microsoft 365 environment. Several workstations need hardware upgrades to better support resource-heavy applications like Bluebeam. Additionally, the company currently lacks structured onboarding/offboarding SOPs, documented IT policies, asset tracking, centralized admin credential storage, full endpoint and Microsoft 365 backup coverage, remote IT support, website deployment, and a formal helpdesk system. A proper knowledge transfer from the current IT manager is still required and mandatory to ensure a smooth transition and prevent any disruption to ongoing operations. Overall, developing a comprehensive IT strategy and executing a phased modernization plan will be essential to support long-term growth, security, and scalability.

II. OBJECTIVES & SCOPE

This report aims to identify key technological gaps within SLB's current IT environment as Solubon Ltd. merges with the organization. The goal is to ensure operational continuity, improve infrastructure, and support future scalability. The scope includes hardware, software, cybersecurity, endpoint management, Microsoft 365 ecosystem, and user support processes.

III. CURRENT STATE ASSESSMENT

Note: A complete inventory and full access list are still required from the outgoing IT manager. The following reflects currently known components from the 6 Depot St. Office.

- **User Devices:** 7 PC setups with ethernet connection (5 with 16 GB RAM, 2 with more)
- **Wi-Fi:** WPA3 security standard in place.
- **Network Hardware:** Patch panel, switches, two Spectrum modems (on floor), UniFi firewall.
- **Antivirus & Endpoint Security:** Microsoft Defender v2 (365); McAfee on some PCs.
- **Printers:** Two current printers; one confirmed as Brother MFC-L3710CW.
- **Backup:** Barracuda for general backup; unclear coverage of MS365 and endpoints.
- **Microsoft 365 Apps:** Outlook, Teams, SharePoint, OneDrive, MFA (Microsoft Authenticator).
- **Website:** Currently empty.
- **Administrative Access:** Transition to Alexandra in progress.

IV. IDEAL FUTURE STATE

- All workstations memory upgraded and optimized for workload.
- Unified endpoint protection with centralized management.
- VPN implemented across all devices (including mobile/iOS).
- Fully integrated Microsoft 365 environment with automation and AI integration.
- Documented IT policies, access control, and asset tracking.
- Website is deployed with domain and DNS managed.
- New user SOP training for software.
- Centralized helpdesk ticketing for users.
- 2 MFPs (Multifunction Printers).
- Full coverage of endpoint and Microsoft 365 backups + disaster recovery plan

V. GAP ANALYSIS TABLE

Note: This gap analysis reflects findings from the SLB office located at 6 Depot St only. The Manhattan site will require a separate audit for full inclusion.

Gap Severity Legend

🔴 **High** – Critical issue; requires immediate action

🟡 **Moderate** – Important but not urgent; needs attention soon

🟢 **Low** – Minor gap; monitor or improve over time

Category	Current Status	Ideal State	Gap Severity	Notes
User Hardware	5 of 7 PCs at 16GB RAM; some lag on Bluebeam	All workstations at 32GB+ or SSD optimized	🟨	Upgrade RAM on 2 PCs + optimize for Bluebeam
Network Security	WPA3 Wi-Fi, UniFi firewall, no VPN	WPA3 and VPN + mobile VPN support	🟥	May need to replace basic Spectrum routers to support Cisco AnyConnect VPN integration
Microsoft 365 Integration	Outlook, Teams, SharePoint, OneDrive used, but not fully leveraged	Seamless integration across all Microsoft 365 apps with productivity workflows, automation, and AI capabilities (where applicable)	🟨	Need to conduct user training to improve file sharing, collaboration, and task flow efficiency
Endpoint Protection	Defender v2 + McAfee on some devices	Unified Defender or premium antivirus	🟩	Standardize endpoint security

Backup Coverage (Data & M365)	Barracuda in place; 365 backup unclear	Confirmed 365 + endpoint backups, as well as a proper disaster recovery plan	🟥	MS365 + endpoint backup plan missing/uncertain
Network Infrastructure	Patch panel with 2 switches and 2 Spectrum routers; no known on-premises servers	Documented and labeled network setup with clear diagrams and secure equipment	🟩	Visually in working order, but needs cable labeling, port mapping, and equipment security + elevation off floor
Printers & Peripherals	2 basic printers; one is Brother MFC-L3710CW	2 all-in-one scan/fax/print models	🟩	Recommend Brother MFC-L8905CDW for best value MFP
Device & Software Inventory	No formal inventory list or tracking of hardware, software, or licenses	Centralized and regularly updated inventory with asset tags and license tracking	🟨	Build and maintain an inventory spreadsheet to track devices, software, and renewals
Website & Domain	Empty website	Functional website	🟥	Need to develop and deploy website + manage domain and DNS
IT Documentation	No formal documentation of processes, credentials, or systems	Centralized internal documentation covering SOPs, network configs, credentials, and support procedures	🟥	Major gap in knowledge retention, must create internal IT knowledge base including admin credentials, onboarding/offboarding steps, and troubleshooting
New User Onboarding SOP	No standardized onboarding process	Documented and repeatable onboarding process with checklist +	🟥	Create a formal SOP that includes account setup, software training, device prep,

		account provisioning	🟥	email, MFA, and permissions
User Access Controls/Permissions	File sharing and SharePoint permissions are inconsistent across users	Role-based access controls with clear permission levels and audit trails	🟨	Conduct access review and implement standard group/role permissions in SharePoint and Teams to ensure least privilege access policy
Remote Access Policy	No formal policy for remote device access or data protection	Documented policy outlining VPN usage, MFA, remote work expectations, and device security rules	🟨	Draft and enforce a remote access policy as VPN gets implemented
Software Licensing Compliance	No centralized tracking of software licenses or subscription expirations	Regularly updated license inventory covering M365, Bluebeam, Adobe, and antivirus	🟩	Create a license tracking sheet to manage multiple software subscriptions
Remote IT Support Software	No software in place for remote troubleshooting or unattended access	Secure remote access tool deployed to support users offsite (e.g., AnyDesk, TeamViewer)	🟩	Implement reliable and lightweight remote support software with encryption and unattended access options
IT Monitoring & Alerts	No centralized monitoring or real-time alerts for system health or backups	Active monitoring for backup failures, endpoint threats, and system health using Defender/Barracuda tools	🟨	Configure alerts via Microsoft Defender, Barracuda, or integrate with monitoring platform for visibility

VI. FINDINGS & RECOMMENDATIONS

- Implement a VPN for all user devices for remote connectivity + define policies.
- Standardize antivirus (remove McAfee, use Microsoft Defender as primary antivirus).
- Upgrade RAM on underpowered machines, especially for Bluebeam users.
- Replace printers with two multifunction fax/scanner/printers.
- Develop and launch website and manage domain/DNS.
- Audit network setup; label cables, ports, and devices.
- Ensure MS365 backups are included under Barracuda coverage.
- Create SOPs for onboarding, offboarding, troubleshooting, and daily procedures.
- Document all IT credentials and admin passwords in secure, centralized access.
- Train staff on Microsoft 365 app integrations and Power Automate.
- Adopt a ticketing system (e.g., Freshdesk, Spiceworks) to manage support.
- Track and manage software licenses and subscriptions.

VII. ACTION PLAN / NEXT STEPS

Short-Term (0–2 Weeks)

- Complete admin transitions and extensive knowledge transfer
- Create full hardware inventory list
- Begin credential documentation
- Validate MS365 backup coverage
- Begin gathering software license data, subscription plans and support information
- Log any license renewals, scheduled maintenance, and vendor support tasks
- Initiate VPN setup and define remote access policy
- Upgrade remaining users' PC RAM
- Review SharePoint/Teams permissions and set privileges

Mid-Term (3–6 Weeks)

- Replace both printers with best value MFPs

- Audit network infrastructure and complete physical labeling
- Train staff on Microsoft 365 best practices
- Standardize antivirus deployment
- Develop and launch company website
- Implement helpdesk/ticketing platform
- Introduce remote connect IT support software (e.g., AnyDesk, TeamViewer)

Long-Term (6+ Weeks)

- Implement monitoring or alerting system for security and backup status (e.g., Microsoft Defender portal)
- Review long-term internet bandwidth needs and negotiate better ISP terms if needed
- Create scalable onboarding/offboarding SOPs
- Introduce monthly reporting on backup status and system health
- Conduct quarterly IT review for supervisors
- Explore Azure Active Directory or hybrid cloud options

VIII. KNOWLEDGE TRANSFER NEEDS

A full knowledge transfer is still pending from the current IT administrator. This should include:

- Complete hardware inventory (names, models, serial numbers, IP addresses)
- Network topology/schematic
- Full Microsoft 365 licensing and admin access documentation
- Disaster recovery plan and business continuity procedures
- Software subscription list (M365, Bluebeam, Adobe, antivirus, etc.)
- All admin credentials (routers, firewalls, cloud services, software portals)
- Current backup configurations and coverage areas (Barracuda, MS365, endpoints)
- Warranty and support contract info (hardware/software)
- Support contacts: ISP, Dell, Logitech, Motorola, Microsoft, Spectrum, Barracuda
- Building management contact information (for power/weather issues)
- Confirmation of UPS (Uninterruptible Power Supply) presence and configuration