✅ LARGE SMB CHECKLIST — YES/NO SHORTHAND VERSION
(Full deep-dive — fast prompts + quick directions)

🟦 A. Business Info
1–7. Business info / contacts / policies requested
→ Ask for: Business name, industry, contact, # employees, IT provider, date, policies (IR/BCP).
YES/NO for each (or N/A)

🔵 B. Network / Wi-Fi (20+ checks)
8. Router brand/model
→ Look at router label.
DONE
9. ISP-provided router?
→ Ask.
YES/NO
10. Router firmware updated
→ Router UI → Firmware/Update tab
YES/NO/UNKNOWN
11. Router admin password changed
→ Ask “Was default changed?”
YES/NO
12. WPA2/WPA3 in use
→ Router UI → Wi-Fi → Security Mode
YES/NO
13. Guest Wi-Fi exists
→ Check SSID list on phone or router
YES/NO
14. Guest Wi-Fi isolated
→ Router → Guest → “Access LAN” OFF
YES/NO
15. VLANs used
→ Router UI → Network/VLANs
YES/NO
16. SSID broadcasting behavior
→ Router UI → Hide SSID?
YES/NO
17. Wi-Fi password complexity
→ Ask owner: simple vs long/random
YES/NO
18. WPS disabled
→ Router → WPS → OFF
YES/NO
19. UPnP disabled
→ Router → Advanced → UPnP → OFF
YES/NO
20. Firewall enabled
→ Router → Firewall/Security → ON
YES/NO/UNKNOWN
21. External admin disabled
→ Router → Remote Management → OFF
YES/NO
22. DNS settings secure
→ Router → DNS (Cloudflare/Google/ISP)
→ If ISP/Default = OK, but note
YES/NO
23. DHCP scope reviewed

→ Router → LAN/DHCP
→ Look for weird devices
DONE/NOT DONE
24. Unknown devices present
→ Router → Connected Devices
YES/NO
25. IoT devices isolated
→ Ask: “Are cameras/printers on their own network?”
YES/NO

🟣 C. Workstations / Devices (15+ checks)
Choose one main PC + ask about rest.
26. Total workstation count
→ Ask
27. Endpoint management used?
→ Ask if IT manages patches centrally
YES/NO
28. Windows Update current
→ PC: Settings → Update
YES/NO
29. Antivirus centrally managed
→ Ask: “Is AV managed by IT?”
YES/NO
30. BitLocker enabled
→ PC: Manage BitLocker
YES/NO
31. Auto-lock enabled
→ Settings → Accounts → Sign-in options
YES/NO
32. Local admin restricted
→ Computer Management → Groups → Administrators
YES/NO
33. Shared logins found
→ Ask: shared accounts?
YES/NO
34. Unsupported OS present
→ Settings → System → About
→ Windows 7/8?
YES/NO
35. Software patching routine
→ Ask: “How often do you update business apps?”
YES/NO
36. USB unrestricted
→ Ask: “Can staff plug in any USB?”
YES/NO
37. RDP enabled
→ SystemPropertiesRemote.exe
YES/NO
38. RDP brute-force logs found
→ Event Viewer (Security) → 4625 spikes
YES/NO/NOT CHECKED
39. Password manager used
→ Ask
YES/NO
40. Local firewall enabled

→ Windows Security → Firewall
YES/NO

🟠 D. Servers & Backups (15+ checks)
41. Server present
→ Ask / observe
YES/NO
42. Server OS version
→ Check or ask
SUPPORTED/UNSUPPORTED
43. Backups scheduled
→ Ask: frequency?
YES/NO
44. Backups offsite/cloud
→ Ask: cloud, drive rotation, etc.
YES/NO
45. Backup encrypted
→ Ask IT or owner
YES/NO/UNKNOWN
46. Backup integrity tested
→ Ask: “Ever restored from backup?”
YES/NO
47. Shadow copies enabled
→ Server Manager (if applicable)
YES/NO/NOT CHECKED
48. Disaster recovery (DR) plan exists
→ Ask
YES/NO
49. Server shares audited
→ Check sample share → Properties → Security
DONE/NOT DONE
50. Overly permissive shares
→ Check “Everyone” or broad groups
YES/NO
51. Critical data location known
→ Ask: “Where do you store most important files?”
YES/NO

🟡 E. Accounts / Access Control (10+ checks)
52. Unique accounts per employee
→ Ask
YES/NO
53. Password complexity enforced
→ Ask/IT
YES/NO
54. Password rotation policy
→ Ask
YES/NO
55. MFA on email
→ Ask
YES/NO
56. MFA on admin accounts
→ Ask IT or owner
YES/NO
57. Inactive accounts removed

→ Ask: offboarding process?
YES/NO
58. Default accounts disabled
→ PC: Users → Guest/Admin disabled?
YES/NO
59. Group memberships reviewed
→ Ask IT: “Ever audit permissions?”
YES/NO
60. Privilege creep observed
→ Does everyone have too much access?
YES/NO
61. Service accounts documented
→ Ask
YES/NO/NOT DOCUMENTED

🟢 F. Email / Cloud Security
62. Email provider (M365/Google/etc.)
→ Ask
NAME
63. MFA required for staff
→ Ask → “Do all staff use MFA?”
YES/NO
64. Spam/phishing filtering enabled
→ Ask / check admin center if allowed
YES/NO
65. Suspicious forwarding rules
→ If allowed: Gmail/M365 admin → check rules
YES/NO/NOT CHECKED
66. External sender tagging enabled
→ [External] tag?
YES/NO
67. DMARC/SPF/DKIM configured
→ Ask IT or check DNS if you have permission
YES/NO/UNKNOWN
68. Password reset policies reviewed
→ Ask owner
YES/NO

🟤 G. Business Processes (10+ checks)
69. Cybersecurity training done
YES/NO
70. Phishing simulations done
YES/NO
71. Incident Response Plan documented
YES/NO
72. Business Continuity Plan documented
YES/NO
73. Vendor access restricted
→ Ask: “Do vendors have login access?”
YES/NO
74. Onboarding procedure documented
YES/NO
75. Offboarding procedure documented
YES/NO
76. Personal device policy exists
YES/NO

77. Remote access policy exists
YES/NO

🟣 H. Physical Security (5 checks)
78. Server/network closet locked
YES/NO
79. Networking equipment secured
YES/NO
80. Cameras secured
→ Ask or observe
YES/NO
81. No sensitive paperwork exposed
YES/NO
82. Workstations not exposed to public
YES/NO

📝 I. Summary Notes (final items)
83. High-severity risks (list)
84. Medium-severity risks
85. Low-severity risks
86. Quick wins
87. Long-term improvements
88. Owner concerns
89. Follow-up scheduled
90. Anything unusual found