STRONDEX

Cyber Insurance Readiness — Top 10 Controls

The highest-impact controls, pulled from our 47-point Cyber Insurance Readiness checklist.

Start here. These are the controls that block the most risk (and the ones auditors and cyber-insurance carriers ask about first). Work top-down — severity is highest at the top.

1	CRITICAL	**Require multi-factor authentication on every email account.** **Verify:** Turn on MFA for all mailboxes (in Microsoft 365, enforce it via a Conditional Access policy or Security Defaults; in Google Workspace, enforce 2-Step…
2	CRITICAL	**Require MFA for all remote access — VPN, RDP, and SSH.** **Verify:** Place every remote-access path behind MFA (VPN client, RDP gateway, SSH bastion or jump host).
3	CRITICAL	**Require MFA for every privileged and administrator account.** **Verify:** Enforce MFA on all admin roles — domain admins, M365 Global Admins, server local admins, and SaaS admin consoles.
4	CRITICAL	**Require MFA for all cloud service consoles (AWS, Azure, M365 admin).** **Verify:** Enable MFA on every cloud root/owner and admin login — AWS root and IAM users, Azure/Entra admins, M365 admin center.
5	CRITICAL	**Take offline or immutable backups at least weekly.** **Verify:** Confirm backups run at minimum weekly to media that ransomware can't reach — immutable cloud storage, object lock, or offline media.
6	CRITICAL	**Store backups separately from production — offsite or in the cloud.** **Verify:** Ensure at least one backup copy lives outside the production environment so a single breach can't destroy both.
7	CRITICAL	**Test backup restoration at least once in the last 12 months.** **Verify:** Perform an actual test restore — recover a file set or system and confirm it works; a backup you've never restored is not a backup.
8	CRITICAL	**Use no shared or generic admin credentials — each admin has a unique account.** **Verify:** Eliminate shared logins; give every administrator a named, individual account so actions are attributable.
9	CRITICAL	**Change default vendor passwords on all systems and devices.** **Verify:** Replace factory-default credentials on firewalls, switches, NAS, cameras, printers, and appliances.
10	CRITICAL	**Don't use admin accounts for day-to-day work.** **Verify:** Give each admin a separate standard account for routine tasks (email, browsing) and reserve privileged accounts for administration only.