OBSIDIAN RIDGE

PROVIDED BY

Pass your cyber insurance application

Eight controls the forms ask about, and what a yes needs behind it

Give this to a client before they fill in a cyber application. Each line is a control that current small-business cyber applications ask about, the question as one carrier prints it, and the evidence a yes needs. Answer yes only where you can show that evidence.

In Travelers v. ICS (2022), the insured had MFA on its firewall and nowhere else. A federal court entered judgment rescinding the policy. (Source: Lockton, global.lockton.com)

CONTROL	THE FORM ASKS	A YES NEEDS
☐ **MFA on email, remote access and admin accounts**	“For which of the following services do you enforce Multi-Factor Authentication (MFA)?” Coalition, New Business Cyber Application, Q6 The form then lists email, remote access (VPN, RDP), and admin or privileged accounts, one line each.	An export from Microsoft 365 or Google Workspace showing MFA enforced for every user, the remote-access settings showing it there too, and a list of admin accounts with their MFA status.
☐ **EDR or MDR on every computer, servers included**	“Do you use an endpoint detection and response (EDR) product across your enterprise?” The Hanover, Ransomware Supplemental Application, Q9 The follow-up asks whether it is tied to a continuous monitoring platform and process.	The device count from the EDR console matched against the device inventory, workstations and servers both, and the name of whoever watches the alerts around the clock.
☐ **Backups kept offline or immutable, locked with MFA, and restore-tested**	“Which of the following are in place for your backup solution(s)?” Corvus, Smart Cyber Insurance Application v3.2, Q10b The choices include an offline or air-gapped copy, immutable backups, and MFA required for access to backups.	Backup settings showing an offline or immutable copy, MFA on the backup console with credentials separate from the office network, and a dated test restore from the last 12 months. OneDrive or Dropbox sync is not a backup, and Beazley asks about that separately.
☐ **Phishing training, with simulated phishing emails**	“Do you proactively use Phishing simulation testing on employees?” Fusion MGA, Cyber Insurance Application, Q22	Training completion records for every staff member and dated results from simulated phishing campaigns. Include the people who pay invoices and send wires.
☐ **A written call-back rule for wire and payment-change requests**	“When a vendor or supplier requests any change to its account details (including routing numbers and account numbers), do you confirm requested changes via an out-of-band authentication (a method other than the original means of request)?” Beazley, Cyber Application F00863, Q21	A written procedure: every payment or bank-detail change is confirmed by calling a number already on file, never one taken from the request, at any dollar amount. Add proof that the people who move money were trained on it.
☐ **A deadline for critical patches**	“In what time frame do you install critical and high severity patches across your enterprise?” The Hanover, Ransomware Supplemental Application, Q14 It is a write-in. Fusion asks the same thing as a yes or no at 30 days from vendor release.	A written patch standard that states the deadline in days, and a report from the device-management tool showing which machines are current.
☐ **No end-of-life software on the network**	“Do you use any end-of-life software within your systems or network infrastructure?” Fusion MGA, Cyber Insurance Application, Q44 A yes leads to two more: is it connected to the internet, and has extended support been bought.	An inventory of operating systems and major applications showing each is still supported by its vendor. For anything that is not: proof it is off the internet and walled off, or covered by paid extended support.
☐ **Encryption on every laptop**	“Does Named Insured implement encryption on laptop computers, desktop computers, and other portable media devices?” Coalition, New Business Cyber Application, Q3 The answers are No, Yes and Sometimes.	A BitLocker or FileVault report from the device-management tool showing every laptop encrypted, with recovery keys stored centrally.

Obsidian Ridge LLC · 964 High House Rd, PMB 2086, Cary, NC 27513 · (984) 999-7785 · ObsidianRidge.io

September 2026 edition. Questions are quoted from the carrier applications named. Forms change; check the client's current application. A readiness aid, not legal or insurance advice.