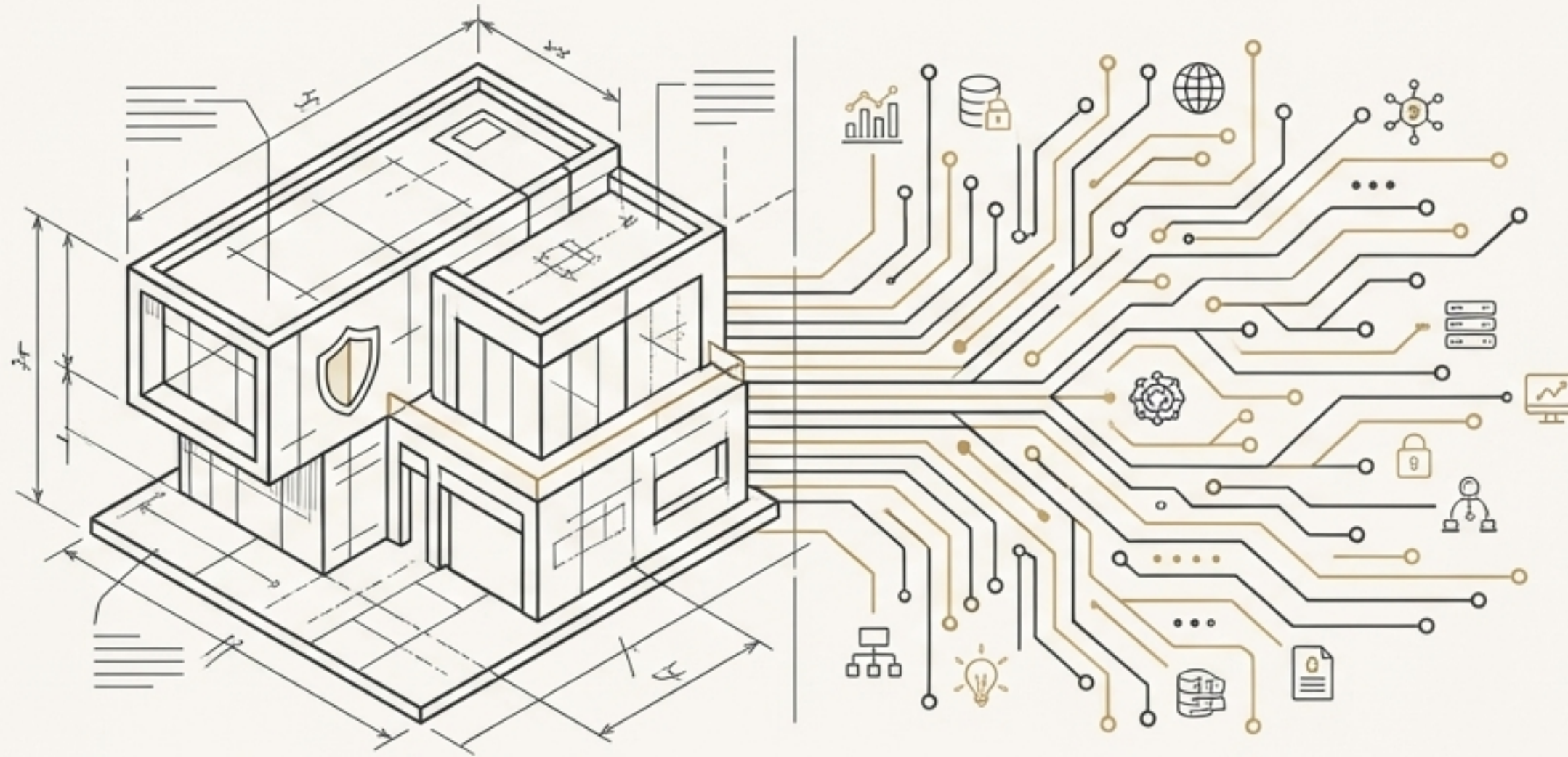


The Solopreneur's Resilience Audit

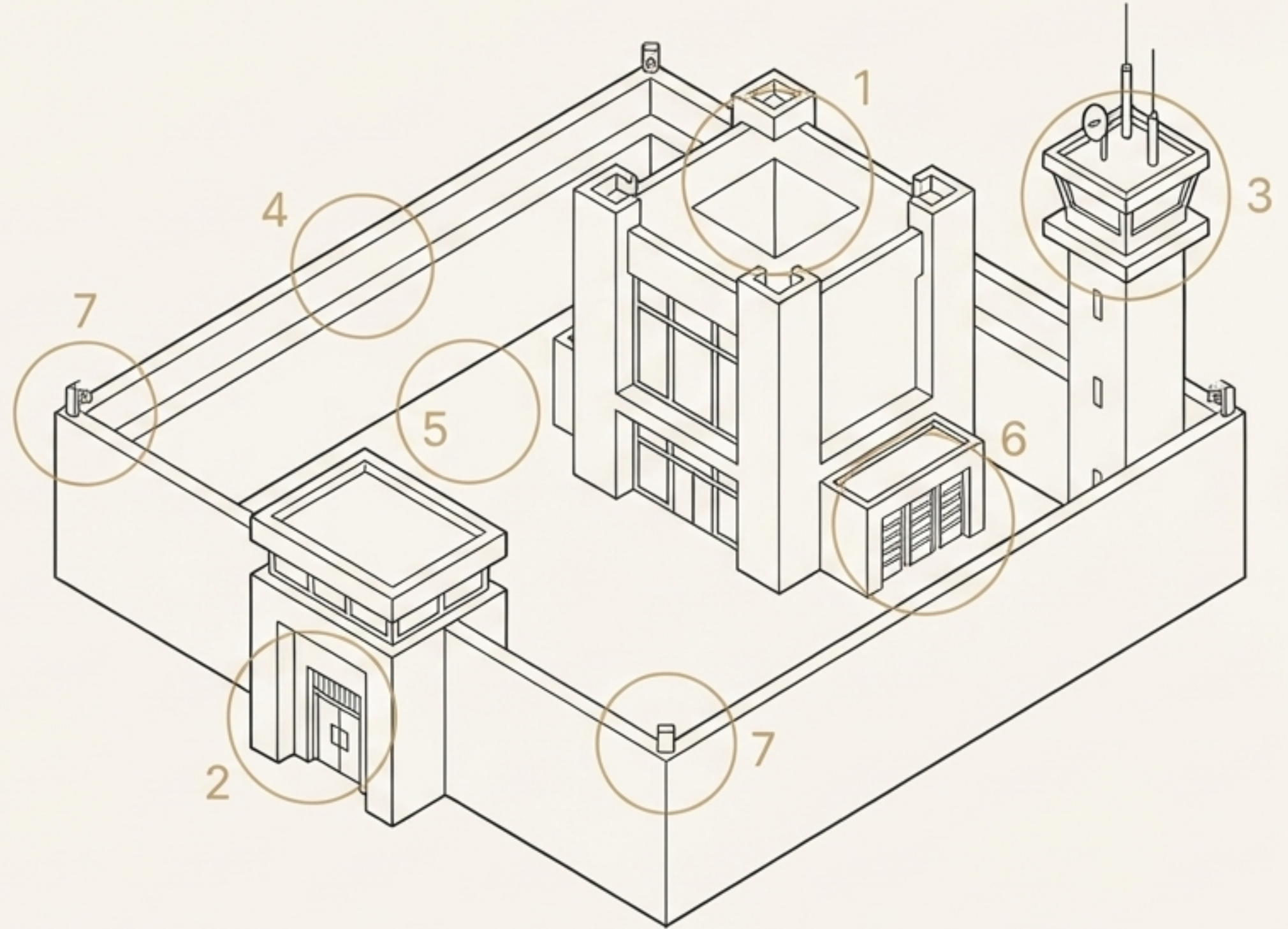
A Cybersecurity Self-Qualification Checklist for Your Business



Your Business is Your Fortress. How Strong Are Its Defenses?

A strong business is built like a fortress, with layers of defense to protect its most valuable assets.

We will audit seven critical areas of your fortress, from the data in your vault to the sentinels on the walls.



This is not about technology.

“It is about whether your business could survive a cyber incident and respond professionally if one occurs.”

This audit is designed to assess your business's core resilience. Each question addresses a critical point of failure that can impact your revenue, reputation, and ability to operate.





1. The Vault: Computer Compromise & Encryption

If your fortress was physically breached, is your most valuable asset secure?

- Do you understand the impact if your computer was lost, stolen, or hacked?
- Is your computer encrypted so data is unreadable if compromised?
- Could you restore your work without paying a ransom?

IMPACT OF FAILURE: Business Paralysis & Extortion. Without access to your data or a way to recover it, your operations halt, and you become a target for ransom demands.



2. The Gates: Email & Cloud Account Compromise

Are your communication channels secure, or can an imposter command your resources?

- Do you understand the impact of unauthorized email or cloud account access?
- Could you stop fraudulent emails or file sharing immediately?
- Do you understand the reputational impact on clients if your accounts are used maliciously?

IMPACT OF FAILURE: Reputational Collapse. Compromised accounts erode client trust, expose sensitive information, and can make you liable for damages caused by fraudulent communications.

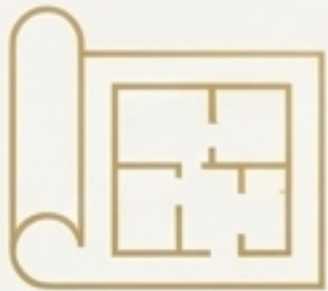


3. The Watchtower: Fraud Detection Awareness

Can you spot an enemy in disguise before they enter the gates?

- Can you identify phishing and impersonation attempts?
- Do you understand common attacker tactics designed to manipulate you?
- Do you rely on a defined process for verifying requests, not instinct alone?

IMPACT OF FAILURE: Financial Theft & Deception. A single moment of misplaced trust can lead to direct financial loss, fraudulent wire transfers, and credential theft.



4. The Battle Plan: Incident Response Readiness

When an alarm sounds, do you have a plan, or will you descend into chaos?

- Do you have written response steps to follow in a crisis?
- Do you know who to contact immediately for technical, legal, or other support?
- Do you know how to resume operations safely without re-introducing the threat?

IMPACT OF FAILURE: Uncontrolled Damage & Prolonged Downtime. Without a plan, small incidents escalate, evidence is lost, and recovery takes exponentially longer, costing you more money and clients.



6. The Sentinels: Detection & Monitoring

Do you have active patrols, or do you wait for a citizen to report a fire?

- Would you know if suspicious activity occurred on your network or accounts?
- Are alerts or active monitoring in place to flag potential threats?

IMPACT OF FAILURE: Undetected Compromise. Attackers can operate inside your systems for months, stealing data and planning larger attacks, while you remain completely unaware.



7. The Night Watch: 24/7 Oversight








Who is watching over the fortress while you sleep?

- Does someone or something monitor your computer, email, and cloud 24/7?
- Are you truly the sole line of defense against a constant barrage of automated attacks?

IMPACT OF FAILURE: Inevitable Breach. A single-person defense is easily overwhelmed. Automated, around-the-clock attacks will eventually succeed if no one is watching.

Your Resilience Scorecard: A Clear View of Your Vulnerabilities

The source material is explicit: "If you answer "No" or "I'm not sure" to any question below, your business is exposed."
Review your answers to the seven audit points. Each represents a critical vulnerability in your fortress's defenses.

	The Vault	<input checked="" type="checkbox"/> SECURE	<input type="checkbox"/> VULNERABLE
	The Gates	<input checked="" type="checkbox"/> SECURE	<input type="checkbox"/> VULNERABLE
	The Watchtower	<input checked="" type="checkbox"/> SECURE	<input type="checkbox"/> VULNERABLE
	The Battle Plan	<input checked="" type="checkbox"/> SECURE	<input type="checkbox"/> VULNERABLE
	The Alliance (Breach Notification)	<input checked="" type="checkbox"/> SECURE	<input type="checkbox"/> VULNERABLE
	The Sentinels	<input checked="" type="checkbox"/> SECURE	<input type="checkbox"/> VULNERABLE
	The Night Watch	<input checked="" type="checkbox"/> SECURE	<input type="checkbox"/> VULNERABLE

Reinforcing Your Fortress

Just because you're by yourself, doesn't mean you have to do it by yourself. Glacier Cybersecurity provides the enterprise-grade reinforcements needed to secure your data, your clients, and your reputation.

**Enterprise Services For
The Solopreneur.**

Mapping Vulnerabilities to Reinforcements

Fortress Vulnerability



The Vault
(Computer Compromise)



The Gates
(Email & Cloud Compromise)



The Watchtower
(Fraud Detection)



The Battle Plan
(Incident Response)



The Sentinels & Night Watch
(Detection & Monitoring)

Glacier Reinforcement

Endpoint Detection & Response

Email Protection, Cloud Identity
Threat Detection

Training & Education

Incident Response, WISP
(Written Plan)

24/7/365 Monitoring
Services

A Complete Arsenal for Your Defense

■ **Cybersecurity Assessment**

Our experts assess your vulnerabilities and provide a customized security plan.

■ **Endpoint Detection and Response**

We monitor your computer 24/7/365 to handle any threat immediately.

■ **Cloud Identity Threat Detection and Response**

Our solutions ensure your cloud data is safe, no matter where it's stored or accessed.

■ **Email Protection**

Crucial protection to stop phishing, the cause of over 80% of breaches.

■ **Incident Response**

In the event of a breach, our team helps you contain the damage and get back on track.

■ **Training & Education**

Comprehensive programs to help you understand and prevent cyber attacks.

■ **WISP (Written Information Security Plan)**

We work with you to create the written security plan most industries require.

Built for Trust, Not Complexity

Our mission is to empower solo professionals to confidently protect their clients, their data, and their reputations through clear, accessible, and effective cybersecurity solutions.

We exist to bridge the gap between enterprise-grade protection and the real-world needs of independent practitioners — delivering compliance-ready security that's built for trust, not complexity.

The Inevitable Choice: Panic or Preparedness

Cybersecurity is not about stopping every attack. It is about limiting damage, protecting trust, and staying in business.

■ Unprepared Businesses Panic



■ Prepared Businesses Recover



The strength of your business tomorrow depends on the preparations you make today.

Secure Your Fortress Today

Get started with a customized Cybersecurity Assessment.



GLACIER CYBERSECURITY



Website: <https://glaciercybersecurity.com>



Email: info@glaciercybersecurity.com



Social: Find Us On LinkedIn