

# Six-Step Cybersecurity Checklist

A quick yes or no self-check across the six steps of a complete cybersecurity program, with the options to consider at each step.

## Step 1: Know where you stand

| Yes                      | No                       | Check                                                     |
|--------------------------|--------------------------|-----------------------------------------------------------|
| <input type="checkbox"/> | <input type="checkbox"/> | We have had an independent security test in the last year |
| <input type="checkbox"/> | <input type="checkbox"/> | We test before renewals, acquisitions and new locations   |
| <input type="checkbox"/> | <input type="checkbox"/> | Someone owns fixing what tests find                       |

**Options to consider:** Internal scans, insurer scans, one-time pen test, recurring independent testing

## Step 2: Prevent

| Yes                      | No                       | Check                                                  |
|--------------------------|--------------------------|--------------------------------------------------------|
| <input type="checkbox"/> | <input type="checkbox"/> | MFA with conditional access on every account           |
| <input type="checkbox"/> | <input type="checkbox"/> | Email filtering plus phishing training                 |
| <input type="checkbox"/> | <input type="checkbox"/> | EDR on every device, watched 24/7                      |
| <input type="checkbox"/> | <input type="checkbox"/> | Managed firewall at every site; no open remote desktop |
| <input type="checkbox"/> | <input type="checkbox"/> | Patches verified, not assumed                          |
| <input type="checkbox"/> | <input type="checkbox"/> | Domain locked, DNS filtered, website monitored         |

**Options to consider:** Do it yourself, platform bundle, or a managed stack

## Step 3: Detect and respond

| Yes                      | No                       | Check                                                |
|--------------------------|--------------------------|------------------------------------------------------|
| <input type="checkbox"/> | <input type="checkbox"/> | Someone watches alerts nights, weekends and holidays |
| <input type="checkbox"/> | <input type="checkbox"/> | Containment actions are pre-approved in writing      |
| <input type="checkbox"/> | <input type="checkbox"/> | We know who responds on site at each location        |
| <input type="checkbox"/> | <input type="checkbox"/> | We know how incident response is paid for            |

**Options to consider:** IR firm retainer, insurer panel firm, or MDR with incident response included

## Step 4: Govern and prove

| Yes                      | No                       | Check                                                  |
|--------------------------|--------------------------|--------------------------------------------------------|
| <input type="checkbox"/> | <input type="checkbox"/> | We have a current WISP and incident response plan      |
| <input type="checkbox"/> | <input type="checkbox"/> | Leadership has run a tabletop exercise                 |
| <input type="checkbox"/> | <input type="checkbox"/> | Evidence is ready for insurers, auditors and customers |

**Options to consider:** Answer as asked, one-time consultant project, or an ongoing vCISO-led program

## Step 5: Recover

| Yes                      | No                       | Check                                                                   |
|--------------------------|--------------------------|-------------------------------------------------------------------------|
| <input type="checkbox"/> | <input type="checkbox"/> | At least one backup copy is off site and out of reach of admin accounts |
| <input type="checkbox"/> | <input type="checkbox"/> | Microsoft 365 or Google Workspace is backed up separately               |
| <input type="checkbox"/> | <input type="checkbox"/> | We have timed a full restore                                            |
| <input type="checkbox"/> | <input type="checkbox"/> | Restore order is written into the IR plan                               |

**Options to consider:** Local, cloud, or hybrid backup with tested continuity

## Step 6: Converged

| Yes                      | No                       | Check                                                          |
|--------------------------|--------------------------|----------------------------------------------------------------|
| <input type="checkbox"/> | <input type="checkbox"/> | Cameras and door controllers are on a separate network segment |
| <input type="checkbox"/> | <input type="checkbox"/> | Device firmware is updated on a schedule                       |
| <input type="checkbox"/> | <input type="checkbox"/> | Installer remote access uses MFA and is logged                 |

**Options to consider:** Separate integrator, segmented and monitored by IT, or one converged partner

## Who should run it?

| Model            | Fits when                                                                                     |
|------------------|-----------------------------------------------------------------------------------------------|
| In-house         | You can staff security around the clock.                                                      |
| Co-managed       | You have IT staff who keep daily control and need 24/7 monitoring, testing and a vCISO added. |
| Fully outsourced | You have no internal IT, or want one accountable partner across sites.                        |

Any box marked "No" is a place to start. Bring this sheet to your consultation and BTI will rank the gaps by risk.

**BTI in Arizona:** a Phoenix office colocated with BTI's data center inside the Iron Mountain data center at 615 N 48th St. BTI staff provide on-site service in the Phoenix metro; in Tucson, on-site service is delivered through BTI's contractors. Public buyers can purchase through BTI's GSA contract. For managed security clients, incident response is included in BTI managed security, as defined in your service agreement.

**Book a free consultation**  
[btigroup.com/freeconsultation/](https://btigroup.com/freeconsultation/)

Phoenix IT team: 480-272-8728

BTI Communications Group: over 40 years in business technology, a 24/7 NOC/SOC, and ISO 27001 compliant policies and controls. This checklist is general guidance, not legal or insurance advice.