PCC LEARNING CENTER

Business IT & Cybersecurity Health Check

A practical self-assessment for business leaders

Use this 24-question screening tool to identify strengths, visibility gaps, and priorities across technology management, cybersecurity, access, continuity, and employee preparedness.

How to use this health check

- Answer based on what is consistently in place today - not what is planned.
- Treat every Not Sure response as a visibility gap that needs an owner.
- Score each section, then choose a small number of concrete priorities.
- Revisit the assessment after meaningful changes or at least annually.

COMPANY

COMPLETED BY

DATE

ROLE

Screening tool only: this does not certify security or replace a technical assessment, audit, legal advice, or insurance guidance.

Business IT & Cybersecurity Health Check

Select one response for each statement. Score **Yes = 2**, **Partly = 1**, and **No or Not Sure = 0**.

		Yes	Partly	No	Not sure
1. Governance and Planning					
1	A specific executive or owner is accountable for technology and cybersecurity risk.	○	○	○	○
2	We maintain a current inventory of hardware, software, cloud services, vendors, and administrator accounts.	○	○	○	○
3	Written IT and cybersecurity policies are reviewed with employees and updated at least annually.	○	○	○	○
4	Leadership reviews technology risks, priorities, lifecycle needs, and budget at least annually.	○	○	○	○
				Section score:	/ 8
2. Identity and Access					
5	Multi-factor authentication is required for email, remote access, administrator, and financial accounts.	○	○	○	○
6	Employees use individual accounts; shared or permanent administrator credentials are tightly controlled.	○	○	○	○
7	Access is based on job responsibilities and sensitive permissions are reviewed at least quarterly.	○	○	○	○
8	A documented process promptly adds, changes, and removes access when employees join, change roles, or leave.	○	○	○	○
				Section score:	/ 8
3. Devices and Network					
9	Company computers and servers use centrally managed endpoint protection and security monitoring.	○	○	○	○
10	Operating systems and common third-party applications are patched through a managed, documented process.	○	○	○	○
11	Firewalls, routers, switches, and wireless equipment are supported, updated, and securely configured.	○	○	○	○
12	Business devices are encrypted and managed, including laptops and mobile devices used outside the office.	○	○	○	○
				Section score:	/ 8

Business IT & Cybersecurity Health Check

Select one response for each statement. Score **Yes = 2**, **Partly = 1**, and **No or Not Sure = 0**.

		Yes	Partly	No	Not sure
4. Email and Data Protection					
13	Business email uses modern filtering plus domain protections such as SPF, DKIM, and DMARC.	○	○	○	○
14	We know where sensitive information is stored, who owns it, and which employees or vendors can access it.	○	○	○	○
15	Employees use approved file-sharing systems rather than personal email or unapproved cloud services.	○	○	○	○
16	Critical cloud data, including Microsoft 365 where appropriate, is covered by an intentional backup strategy.	○	○	○	○
	Section score:				/ 8
5. Backup and Business Continuity					
17	We have written business continuity and cyber incident response plans with named responsibilities.	○	○	○	○
18	Backups are monitored and restoration is tested; at least one protected copy is isolated or immutable.	○	○	○	○
19	Critical systems have documented recovery priorities, acceptable downtime, and acceptable data-loss targets.	○	○	○	○
20	We have practical workarounds for internet, system, facility, or key-vendor disruptions.	○	○	○	○
	Section score:				/ 8
6. People, Response, and Vendors					
21	Employees receive recurring security awareness education and realistic phishing practice.	○	○	○	○
22	Employees know exactly how and where to report a suspicious email, lost device, or possible incident.	○	○	○	○
23	Third-party access is approved, limited, monitored where appropriate, and removed when no longer needed.	○	○	○	○
24	Cyber insurance requirements are reviewed and evidence of required controls is maintained.	○	○	○	○
	Section score:				/ 8

Turn Your Results Into Priorities

Add the six section scores. Higher scores indicate more practices are reported as in place; they do not prove that controls are effective. Count Not Sure answers separately - uncertainty is itself a risk signal.

TOTAL SCORE _____ / 48

NOT SURE COUNT _____

40-48	**Stronger foundation**	Validate effectiveness through testing, evidence, and continuous improvement.
28-39	**Important gaps**	Assign owners and address the highest-impact gaps within the next 90 days.
16-27	**Elevated exposure**	Create a structured remediation plan; avoid treating isolated tools as a complete strategy.
0-15	**Urgent attention or limited visibility**	Seek a professional assessment and establish ownership, inventory, access, backup, and response basics.

My five priority actions

1. _____
2. _____
3. _____
4. _____
5. _____

Need help validating the results or building a practical plan?

Professional Computer Concepts helps Bay Area businesses reduce risk and improve IT operations.

415-897-0078 | www.calpcc.com/lets-talk/