



Secure. Stable. Supported.

SELF-ASSESSMENT TEMPLATE

IT Health Check

An honest look at how well your day-to-day IT is
actually working — support, licensing, devices and
the basics that quietly cost you.

ORGANISATION

COMPLETED BY

DATE

BEFORE YOU START

Bad IT rarely fails. It just wears you down.

Most businesses do not have an IT crisis. They have a slow, steady drip of small problems that nobody has the time to fix properly, and which have quietly become normal.

The printer that only works if you restart it. The new starter who waited a week for an account. The laptop everyone knows is too slow but nobody has replaced. The licences you are fairly sure you are paying for but not using. None of it is urgent. All of it costs.

This template gives you a clear-eyed view of how your IT is actually performing – not in technical terms, but in the terms that matter: time lost, money spent, risk carried.

This is yours to complete. No technical knowledge is required. Some questions may need a word with whoever looks after your IT, and where you do not know the answer, that is itself worth recording.

Answer as things are, not as they should be. The value here comes entirely from honesty. A page of optimistic ticks tells you nothing; a page with eight “unsure” answers tells you exactly where to look.

TWO THINGS TO NOTE

This template refers to Microsoft 365 capabilities throughout, and availability varies depending on your licensing – confirm what your plan includes before assuming either capability or extra cost. It also deliberately overlaps with security in places, because in day-to-day IT the two cannot be sensibly separated.

WHAT THIS TEMPLATE COVERS

01 Support & response

02 Devices & equipment

03 Licensing & spend

04 Starters & leavers

05 Maintenance & monitoring

06 Continuity & key-person risk

Good IT is boring, and that is the point

The measure of healthy IT is not how quickly problems get fixed. It is how few there are to fix.

There is a version of IT support that looks responsive and feels reassuring: things break, someone comes quickly, the problem goes away, everyone is grateful. It is also a sign that something is wrong. A business that needs frequent rescuing has an environment nobody is maintaining.

Healthy IT is unremarkable. Devices are current, updates happen without anyone noticing, new starters work on day one, and the same fault does not recur. The four questions below get at whether yours is in that state.

01 Do the same problems keep coming back?

Recurrence is the clearest sign that symptoms are being treated rather than causes. A fault fixed properly does not return.

02 Does anything only work because of one person?

Passwords in someone's head, a process only they can run, a supplier only they can call. Convenient until they are unavailable.

03 Do you know what you are paying for?

Licences, subscriptions and renewals accumulate quietly. Most businesses are paying for something they stopped using.

04 Is anyone looking after it when nothing is wrong?

Maintenance, updates and monitoring happen between incidents, or they do not happen at all. This is the difference between support and management.

WORTH SAYING PLAINLY

Some findings here will not need a supplier at all. Documenting a process, tidying licences or agreeing who owns what are things a business can do for itself, and they are often the changes that help most.

SECTION ONE

Support & Response

How problems get reported, how quickly they are dealt with, and whether they stay dealt with.

WHO CURRENTLY PROVIDES IT SUPPORT

MONTHLY COST, IF KNOWN

ISSUES RAISED / MONTH

That last figure is worth estimating even roughly. It gives you a baseline to compare against once things improve — and a falling number is the clearest evidence that causes, rather than symptoms, are being dealt with.

Is there one clear way to report a problem?

A single route everyone knows, rather than messaging whoever seems most likely to help.

☐ YES ☐ NO ☐ UNSURE

Do you know how long issues typically take to resolve?

If nobody is recording it, the answer is usually longer than anyone believes.

☐ YES ☐ NO ☐ UNSURE

Do the same problems recur?

The printer, the slow laptop, the system that needs restarting weekly. Recurrence means the cause was never addressed.

☐ YES ☐ NO ☐ UNSURE

Do staff work around problems instead of reporting them?

If people have given up asking, your issue log is not a picture of reality.

☐ YES ☐ NO ☐ UNSURE

Is IT taking up time that belongs to another role?

An office manager or director absorbing IT work is a real cost, just not one that appears anywhere.

☐ YES ☐ NO ☐ UNSURE

Can you reach someone who knows your environment?

As opposed to explaining your setup from scratch each time you make contact.

☐ YES ☐ NO ☐ UNSURE

RECURRING PROBLEMS WORTH LISTING

ProblemHow oftenWho it affects

SECTION TWO

Devices & Equipment

Old and unmanaged devices are the most common source of daily frustration, and the easiest cost to justify fixing.

TypeHow manyOldest isManaged centrally? DesktopsLaptopsPhones / tabletsServersPrinters / scanners

Do you have a list of every device the business owns?

You cannot maintain, secure or budget for equipment nobody has written down.

☐ YES ☐ NO ☐ UNSURE

Is every business-owned device assigned to someone?

A named owner per device makes loss, damage and recovery on departure straightforward. Unassigned kit tends to quietly disappear.

☐ YES ☐ NO ☐ UNSURE

Is any device slow enough to be costing real time?

Five minutes a day lost to a tired laptop is roughly two working days a year, per person.

☐ YES ☐ NO ☐ UNSURE

Is there a replacement plan, or do you replace on failure?

Replacing on failure guarantees the disruption happens at the worst possible moment.

☐ YES ☐ NO ☐ UNSURE

Are devices set up to a consistent standard?

Or does each one reflect whoever configured it, and when?

☐ YES ☐ NO ☐ UNSURE

Do staff use personal devices for work?

Common and often fine, but it needs to be a decision rather than something that simply happened.

☐ YES ☐ NO ☐ UNSURE

Is anything running software past end of support?

Unsupported systems receive no fixes, which makes them a growing liability rather than a saving.

☐ YES ☐ NO ☐ UNSURE

A USEFUL SUM

Take the hourly cost of a member of staff, multiply by the hours a week they lose to slow or faulty equipment, and multiply by 46 working weeks. The figure is usually larger than the cost of the replacement.

SECTION THREE

Licensing & Spend

The section most likely to find money. Subscriptions accumulate quietly and are rarely reviewed once set up.

Subscription / licenceHow manyIn useCostRenews

Does your licence count match your headcount?

Licences for leavers are among the most common wasted costs, and among the easiest to recover.

☐ YES ☐ NO ☐ UNSURE

Is everyone on the right plan for what they do?

Paying for capability people never touch, while others lack what they need, is very common.

☐ YES ☐ NO ☐ UNSURE

Do you know what your Microsoft 365 plan actually includes?

Many businesses already own device management, automation or security features they have never enabled.

☐ YES ☐ NO ☐ UNSURE

Is there anything you pay for and no longer use?

Tools bought for a project, a former supplier's software, a service replaced but never cancelled.

☐ YES ☐ NO ☐ UNSURE

Do you know when your renewals fall due?

Renewals that pass unnoticed remove the opportunity to review or renegotiate.

☐ YES ☐ NO ☐ UNSURE

Is anyone accountable for reviewing IT spend?

Without an owner it only ever moves upward.

☐ YES ☐ NO ☐ UNSURE

SECTION FOUR

Starters & Leavers

How well a business handles arrivals and departures says a great deal about how well its IT is run generally.

TYPICAL TIME TO GET A NEW STARTER WORKING

WHO HANDLES IT

Can a new starter work productively on day one?

Account, email, files, software and a device ready before they arrive, not during their first week.

☐ YES ☐ NO ☐ UNSURE

Is there a written onboarding checklist?

If it lives in one person's memory, something gets missed whenever they are away.

☐ YES ☐ NO ☐ UNSURE

Are leavers' accounts disabled the same day?

Email, files, remote access and any third-party services. Delay here is a genuine security exposure.

☐ YES ☐ NO ☐ UNSURE

Is equipment recovered when someone leaves?

Laptops, phones and access cards, with a record of what came back.

☐ YES ☐ NO ☐ UNSURE

Is a leaver's work handed over properly?

Files, mailbox contents and anything held only in their personal storage.

☐ YES ☐ NO ☐ UNSURE

Are role changes handled as carefully as arrivals?

People who move roles usually gain access and rarely lose any, which is how permissions sprawl.

☐ YES ☐ NO ☐ UNSURE

WHY THIS MATTERS MORE THAN IT LOOKS

Onboarding is a good proxy for the health of everything else. A business that can equip a new starter in an hour has documentation, standard builds and clear ownership. One that takes a week usually has none of the three.

SECTION FIVE

Maintenance & Monitoring

The work that happens when nothing is wrong. This is the difference between IT being managed and merely being fixed.

Are updates applied automatically across all devices?

Operating systems and applications both, without relying on individuals to accept prompts.

☐ ☐ ☐
YES NO UNSURE

Is anything monitoring your systems?

Disk space, failed backups, offline devices, expiring certificates. Problems announced before they bite.

☐ ☐ ☐
YES NO UNSURE

Would you know if a backup had failed?

Silent backup failure is common and is only ever discovered when a restore is needed.

☐ ☐ ☐
YES NO UNSURE

Has a restore been tested in the last year?

An untested backup is an assumption, not a safety net.

☐ ☐ ☐
YES NO UNSURE

Is multi-factor authentication enabled for everyone?

The single most effective control available to most businesses, and usually included in what you already pay.

☐ ☐ ☐
YES NO UNSURE

Is antivirus or endpoint protection active on every device?

Active, current, and with someone actually reading the alerts it produces.

☐ ☐ ☐
YES NO UNSURE

Does anyone review the environment periodically?

A scheduled look at what has changed, what is ageing and what is coming, rather than only reacting.

☐ ☐ ☐
YES NO UNSURE

WHERE MICROSOFT HELPS

Update policies, device compliance and reporting can be enforced centrally through **Intune**, with endpoint protection via **Microsoft Defender** — both often already owned rather than bought.

Availability depends on your Microsoft 365 licence.

SECTION SIX

Continuity & Key-Person Risk

What happens when something fails, or when the person who understands it is unavailable.

Could the business operate if the office was inaccessible?

Not hypothetically – could people work tomorrow, from elsewhere, with what is in place today?

☐ YES ☐ NO ☐ UNSURE

Could the business continue if your internet connection failed?

Now that most systems are cloud-based, the connection is critical infrastructure. A backup route matters more than it used to.

☐ YES ☐ NO ☐ UNSURE

Is there a single person who holds critical knowledge?

Passwords, supplier relationships, how a system works. This is the most common risk in a smaller business.

☐ YES ☐ NO ☐ UNSURE

Are administrator credentials held securely and accessibly?

Shared access should sit in a password manager rather than a notebook, a spreadsheet or someone's personal browser – and someone other than that person must be able to reach it.

☐ YES ☐ NO ☐ UNSURE

Do you have a record of suppliers, contracts and accounts?

Who to call, what the account number is, and what each contract covers.

☐ YES ☐ NO ☐ UNSURE

Is your environment documented at all?

Even a single page listing systems, suppliers and how things connect puts you ahead of most.

☐ YES ☐ NO ☐ UNSURE

Is there a plan for a serious IT failure?

Who is called, who decides, what happens first, and how staff are told.

☐ YES ☐ NO ☐ UNSURE

SINGLE POINTS OF FAILURE

System or knowledgeWho holds itWhat happens without them

MAKING SENSE OF IT

Where you stand

Count the questions you answered “no” or “unsure”. Both matter: one is a gap, the other is a blind spot, and blind spots tend to be the more expensive of the two.

0 – 5

Well run. Focus on the specific gaps rather than changing anything structural, and keep the review habit going.

6 – 14

Typical of a business whose IT has grown without a plan. Most of this is configuration and process rather than expenditure.

15 or more

Your IT is being reacted to rather than managed. Start with backup, MFA and leaver accounts – the three with real consequences.

Mostly unsure

Visibility is the first problem to solve. An hour spent establishing the facts will change every answer above.

THE THREE WORTH DOING FIRST, WHATEVER YOUR SCORE

Confirm your backups run, and restore something

The only test that counts. Everything else on this list is recoverable; data loss frequently is not.



Turn on multi-factor authentication for every account

Usually included in your existing licensing, and it removes the most common route into a business.



Reconcile your licence list against your staff list

This one frequently pays for itself immediately, and it takes an afternoon.



YOUR THREE PRIORITIES

NEXT STEPS

None of this needs to be dramatic.

Most of what this exercise turns up is fixed with configuration, documentation and someone taking ownership – not with new systems or a larger budget.

If you would like a second opinion on what you have found, or help closing the gaps, we are happy to talk it through. No commitment, and no obligation to change who supports you.

And if your IT is in good shape, we will tell you that and leave you to it.

INNOVASYSTEMS

Managed IT support
Microsoft 365
administration
innovasystems.tech

THE GROUP

Innova Technologies Group
Ltd
Hull, United Kingdom
innovagroup.tech
hello@innovagroup.tech

ALSO IN THIS SERIES

Cyber Security Essentials Checklist
Cloud Migration Readiness Template
Process & Automation Opportunity
Finder
Choosing a Technology Partner

FOUR DISCIPLINES, ONE PARTNER

● **InnovaSystems**
Secure. Stable. Supported.

● **InnovaWorks**
Building What's Next.

● **InnovaCloud**
Cloud Without Complexity.

● **InnovaSecure**
Protect What Matters.

Technology That Works. Innovation That Lasts.