Platform 365

Inside an IT Infrastructure Review: what it involves and what it reveals

Most businesses don't have a complete picture of their IT. Environments grow gradually, around the priorities of the day. A new firewall goes in when the old one fails. A switch gets added during a busy week, with the intention of documenting it later. Microsoft 365 licences accumulate as people join, but nobody goes back to clean them up when staff leave. After a few years, the picture is patchy even for the people who set most of it up.

An IT Infrastructure Review is the structured exercise that pulls that picture together. It's an independent assessment of what's running, how well it's working, where the risks are, and what should be prioritised. The output is a working document that gives the business a clear view of its environment and a credible plan for what to do next.

When companies commission a review

We typically see three scenarios.

1. The first is reactive.
Something has gone wrong or come close to it. A server has failed, an email account has been compromised, or an audit has flagged a gap. The business wants an independent view of the wider environment to understand whether the underlying issues run deeper.

2. The second is transitional.
A change is coming, perhaps growth into a new site, a planned migration to the cloud, an upcoming insurance renewal, or a decision to switch IT provider. The review provides the baseline that those decisions can be built on.

3. The third is preventative. Nothing is wrong, nothing is changing, but the leadership team wants to know what they don't yet know. These are often the most useful reviews to commission, because they're done with time to act rather than under pressure.

The areas we assess

A review covers the whole stack: the cabling in the walls, the networking and server hardware, the cloud platforms running on top, and the services that depend on all of it.

Core Infrastructure

Core infrastructure covers the physical environment (data cabling, comms racks, power, and cooling) alongside internet connectivity, the firewall, the local-area network and switching, Wi-Fi, and any on-premises servers. The questions are practical: Is the comms rack in a secure location? Is there a backup internet link? Is the firewall still receiving security updates? Is the Wi-Fi managed by something that supports modern standards? End-of-life hardware is a recurring theme here, particularly firewalls and wireless access points that have quietly slipped past their vendor support dates.

End-User Devices

End-user devices cover desktops, laptops, and printers. We check the operating systems, the endpoint security in use, how updates are delivered (and whether anyone is monitoring whether they land), and whether there's a hardware inventory worth its name. Printers are usually straightforward, especially when they're leased and supported by the supplier. Desktops and laptops are where most of the patching and management gaps tend to show up.

Cloud Services

Cloud services, for most SMEs, means Microsoft 365. We look at subscription mix, licence count against actual users, the security tier in use, and what advanced controls are or aren't switched on. Licence drift, where a business is paying for accounts that should have been removed or paying for Business Standard when Business Premium would be more appropriate, is one of the most common findings and one of the easiest to act on.

Core Services

Core services cover email and file sharing, which sit on top of the cloud platform. The review looks at what product is in use, what security features are available, how email is protected against phishing and malware, and how file data is stored, accessed, and backed up. Backup is worth a separate mention here. Microsoft 365 includes resilience, but a true independent backup is a separate decision, and a surprising number of businesses assume it's already in place when it isn't.

Network Services

Network services cover Active Directory, Group Policy, DHCP, and DNS, the services that hold the network together. These are reviewed for stability, configuration against best practice, and whether they're hosted on infrastructure that has a supported lifecycle ahead of it.

What the report looks like

The deliverable is a single document, usually around fifteen to twenty pages depending on the size of the environment. It opens with an executive summary that names the strengths, the weaknesses, and the headline recommendations. Anyone in the leadership team can read the summary and come away with a clear sense of what the review found.

The detailed sections follow. Each area gets its own page (or two) with the ratings table, the supporting commentary, and the recommendations. The language is written to be readable by a non-technical reader without losing the precision a technical reader expects. Where assumptions have been made, or where access wasn't available during the review, that's stated openly.

At the back of the report is a prioritised recommendations table that pulls every action together in one place, ranked by importance. That's the working list the business can take forward.

Common findings

After enough reviews, certain patterns repeat. None of these are unusual; readers should expect to recognise themselves in at least some of them.

End-of-life hardware

Firewalls, switches, wireless access points, and servers that are still working but no longer supported by the manufacturer. These often pass unnoticed because the business hasn't experienced any direct consequence yet.

Unsupported operating systems

Servers running Windows Server 2008 or 2012, occasionally older. The risk is twofold: no security updates and a higher chance of hardware failure on the box itself.

Manual or USB-based backups

A USB disk taken home each night was reasonable practice a decade ago. It's now a working process that depends on a person remembering, and it offers limited protection against fire, theft, or a forgotten drive.

Single points of failure

A firewall that also provides Wi-Fi, a single switch carrying every connection in the building, an internet line with no failover. These are often choices made for cost reasons that quietly grow into business risks as the environment becomes more reliant on them.

Microsoft 365 licence drift

Paid-for accounts that belong to leavers, the wrong mix of plans, advanced security features sitting unused inside subscriptions the business is already paying for.

Limited centralised management

No hardware inventory, no central record of which devices have which updates, no automated way of pushing third-party patches. Most SMEs manage this informally for years before the gap becomes visible.

Old data on old servers

A legacy file share that nobody quite knows what to do with, sitting on hardware that should have been retired three operating-system generations ago. The data is rarely critical, but it's also rarely entirely unimportant, and it keeps the old server alive long after it should have been switched off.

Turning the findings into action

The report is designed to be useful for the next 18 months, not just the week it lands. Three things tend to make the biggest difference to how it's used.

First, prioritise by importance. Critical items have either a hard deadline (a licence expiry, an end-of-support date) or a level of risk that doesn't justify waiting. They go to the top of the budget conversation. High and medium items follow, planned around the natural rhythm of the business. Low items are good housekeeping and can usually be picked up over time.

Second, use the report as a budgeting tool. The recommendations give finance a concrete list of work to plan around, rather than a vague sense that IT needs investment. It also makes it easier to phase the spend across a financial year.

Third, if there's an existing IT provider, use the report as a conversation. Most good providers welcome the second opinion because it gives them a useful checkpoint and a clearer mandate. A less engaged provider will push back, which is its own kind of useful information.

Who should commission a review

The short answer is any UK SME that hasn't had an independent look at their environment in the last two to three years, particularly where the business has grown, changed, or absorbed another company in that time.

The compliance and insurance angle is becoming a more common driver. The UK government's Cyber Security Breaches Survey 2025/2026 found that 43% of UK businesses identified a cyber breach or attack in the previous 12 months. Cyber insurers have responded, and renewals now involve detailed questions about multi-factor authentication coverage, endpoint detection, patching discipline, backup testing, and incident response readiness. Underwriters increasingly want evidence, such as configuration screenshots, recent test results, and named products with active licences. A structured infrastructure review puts a business in a much better position to answer those questions honestly and in detail, and it surfaces the gaps that would be flagged later.

The same logic applies to Cyber Essentials certification, supplier security questionnaires, and any contract that requires the business to demonstrate basic cyber hygiene. A review gives a business the baseline that those exercises all depend on and surfaces the gaps they would otherwise expose later.

Booking a review

Pricing starts from £1,350, depending on the size and complexity of your environment.

Platform365