The essential IT health check

The 10 killer questions you should be asking about your IT

a ramsac guide

ramsac
at the heart of IT

Organisations depend on the smooth running of their IT – if something goes wrong, chances are the entire company will be affected, but if everything is ticking along nicely work is more efficient, staff frustration is lowered and life is easier.

This guide will give you the 10 simple questions you need to ask to perform your own routine "IT health check" and make sure your technology and information assets are working for, not against, you.

ramsac
at the heart of IT

How quickly can you restore a file - or your whole system?

Most organisations understand the need to run a robust backup. But many feel that once they've made the investment in an online backup or a tape drive, the work is done. In truth, not all backups are created equal, and you need to ask some important questions about your own system.

As with an insurance policy, you really only know how good your backup system is when something has gone wrong. But that's the worst time to find out that your system isn't quite what you hoped it would be!

It's no good running a two-week rotation of tapes if you discover someone deleted a client folder four weeks ago – at the very least you should keep a month-end and year-end tape in a safe somewhere away from site.

In truth, the question isn't 'how good is my backup?' but, rather, 'how effective is my ability to restore?' And as well as running your backup each day, you need to question how frequently you are testing the ability to restore a file, folder or full system, and how long a recovery would take.

If you're running a traditional tape backup, you should consider the following things:

- rotation of tapes
- the process for ensuring tapes are changed daily
- off-site tape storage
- how often snap-shot backups are taken out of the tape rotation and stored permanently off-site

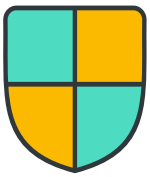
If you're backing up to the cloud, question what's being backed up, where the data is being stored and how quickly you can undertake a significant restore. Cloud backup is brilliant for removing the inconvenience of changing tapes each day, but if you have a significant incident and need to restore your entire shared drive, doing so will take a very long time if you have to restore it file-by-file over a sluggish internet connection.

Also question what's being backed up. It's no good backing up files and not backing up the system itself – if your entire system goes down, it will add days to your recovery time if you can't quickly restore the system settings, server profiles and user info, as well as the files themselves.

We have seen many organisations lulled into a false sense of security after storing all their data on a shared Google drive, only to discover a virus has infected the whole drive and everything has been lost.

Although cloud providers such as Microsoft and Google will have their own backups, they are geared towards recovering from disasters in their systems, not general issues with corrupt, deleted or overwritten files. There are cloud-based systems that back up your cloud files to another source – it's often low cost and low admin. But don't think that just storing files in a cloud makes you watertight; data should always be stored in at least two locations to ensure that if one source fails, you have a 'plan b' to fall back on.

Don't assume that, just because your files are stored in the cloud, you don't need to think about a separate system backup.



How quickly can critical network hardware be repaired or replaced?

If you've ever bought a washing machine from a high street electrical store, you will no doubt have had the awkward conversation about extended warranties. Thankfully, PCs and tablets are now so easily available, and relatively cheap, that there's very little point worrying about long warranty periods. But there are some core parts of your network that are costly to replace, complex to configure and affect everyone's ability to work. For these items, it's important to know that if a part fails you can guarantee a replacement will be on site within a few working hours.

This means that if the motherboard in the server dies, you'll know that a replacement part will be available and will be with you on the same day, reducing your exposure to companywide down time.

Typically, you should ensure that any servers are protected by a manufacturer's warranty, with a four-hour response.

Skimping on warranty cover is generally a false economy. When a machine is under warranty, the manufacturer will continue to hold replacement parts, even if that particular device is no longer made. You will also be at the front of the call out queue. To not have a warranty means you might not source the replacement part or you could wait two days to get an engineer onsite – a costly delay if your whole organisation is unable to work.

Most servers ship with a three-year warranty which can normally be extended to five years, or, in some cases, seven years. Check that your key systems are all covered and that you have a system in place for ensuring you don't miss a renewal date.

When it comes to networking hardware, such as firewalls, routers and switches, you should consider having a spare device, configured in line with the primary device, so that if there is a failure they can quickly be swapped, avoiding network wide downtime.

Are your licences in check?

Keeping track of software can be tricky. Make sure you know whom within your organisation is responsible for ensuring that everything you use is properly licensed. It's not just Microsoft products; think about the line of business applications you use, the creative team's software, your antivirus and back-up products and the systems that you use to run your building, such as door entry and security systems.

Microsoft licensing can be really complicated – it's not just about the licenses for your local PC or laptop, you need to consider all of the servers, and, in some cases, the 'client access licenses' needed for each user that accesses server applications.

If you haven't yet been audited by Microsoft, chances are you will be soon – they are slowly reviewing all UK organisations and a license review can be hard work. Ensure you know what you need and what you have, and check that someone is tracking expiry dates – it can be twice as expensive to renew some licenses if the expiry date has already lapsed.

When we audit an organisation, we find as many people that are over licensed as we do those that are under licensed. You could be paying for more than you need to.

Are you monitoring the network?

Though most modern cars will proactively monitor things such oil levels, tyre pressure, and emissions to catch issues before they cause damage, physical checks and servicing are still essential. You don't wait for your car to break down before you ensure that someone has at least checked under the bonnet – you take it to the dealer for regular assessment and servicing.

Your network should be set up with monitoring tools that automatically alert you to potential risks, such as spikes in disk space, backup failure, failing hardware, attempts by hackers, and devices on the network that haven't got up to date antivirus software, and these alerts should be actioned in a timely manner so that you prevent something small from escalating into a much more serious problem.

There are very few critical events that can't be predicted and therefore prevented, but only if someone is actively managing and monitoring the network.

Who's updating the systems?

We all know how annoying it is when you attempt to close down your laptop to go home, only to receive the message that your machine is downloading 34 updates and must not be switched off. But patches and updates are essential and primarily serve to keep your system safe.

Malicious attacks, system vulnerabilities and performance limiting issues are being discovered by software manufacturers every day, and the patches and updates that you are prompted to download are there to correct those issues or to secure a newly discovered vulnerability. Systems that are not kept up to date are accidents waiting to happen. Malicious users actively scour the internet looking for vulnerable systems, making an unpatched network the equivalent of an open door for a burglar.

You should check who is monitoring user devices and servers to ensure that systems are being kept up to date. When it comes to server updates, these need to be reviewed, managed and installed at a time where the network isn't busy, as they can sometimes require restarts or cause downtime. End-user devices should generally be set to download updates from the network rather than directly downloading from the web, as the latter can cause network delays if all machines start downloading across your internet connection at the same time.

Updates should be planned, controlled, enforced and, most importantly, regular!

How well are you controlling access?

There's no point in putting the best locks on your front door and installing the latest intruder alarm if the last person out of the office at night leaves the door wide open. Access control to your information systems is about great housekeeping – it is essential that you have a good password policy in place, which ensures users regularly change their network passwords with something more complex and secure than 'Password01', but it's also important to make sure that someone is tidying up after users that leave the organisation. Idle user accounts are a hacker's dream, an ideal opportunity to exploit weak passwords and gain access under the radar.

You should run a monthly check on your user directory to query if accounts have passwords that aren't set to expire and how many accounts haven't been accessed for 30 days, as that probably means that someone has left the business but no one has closed down their account.

Also think about who has access – you wouldn't give every member of your team access to your internet banking, but it's amazing how many organisations allow multiple team members to have admin access to the servers.

Remember, if I have admin access to your server, I can see all your files and all your emails.

Think about who really needs which levels of access, and then consider what you do if one of your trusted employees moves on. Review your password policies and ensure that these are being centrally enforced rather than relying on users to voluntarily comply. Consider whether 'two factor authentication' (a system where, for example, a passcode is sent as an SMS to a users mobile device) is appropriate for access to very sensitive data.

How well do you train staff on IT security?

IT security is not just about good investment in technology. You can have a fastidious password policy and the latest firewall technology in place, but all that sensible investment is useless if an employee clicks on a phishing email and reveals their password to a complete stranger.

IT security is 50% infrastructure, and 50% user training. And yet few businesses ensure that their teams regularly receive up-to-date training on good practice and cyber security awareness.

Training should be applied across the board and should be programmed to happen regularly.

The industry changes at a breakneck pace – the threats we're battling today did not exist six months ago, so training should be kept up to date.

When did you last test your business continuity plan?

Though some people find business continuity planning fascinating, most would probably admit it's quite a long way down the list of things they would like to do with their time. But let's assume you've been really organised and developed a companywide plan for how you will respond to an interruption to your day-to-day operations. For starters, well done, you're already one step ahead of most of your competitors! But, if that plan was written 18 months ago and has since been sat gathering dust on the shelf of your server room, chances are it's not quite up to the job.

Organisations change all the time. People come and go; suppliers get reviewed; new technology is implemented; key customers change. A business continuity plan is no different – it should change at the same pace as your business. It's also no good unless the whole team knows how and when to implement it.

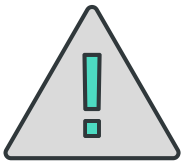
You should schedule in regular 'table top' tests of your BCP, involving different parts of your organisation each time. Think of different scenarios; fire and flood are the obvious ones, but consider a loss of power, loss of access to your building, loss of a key member of your staff, a major supplier going bust… and make sure your plan remains fit for purpose in each scenario.

Our experience is that every time we've tested our plan, we've highlighted changes to make, even if that's just realising that a contact list has become out-of-date.

What are you tolerating?

This question is actually good to ask about your wider organisation too, but, thinking about IT, what is it that you're putting up with, or accepting second best on? How well are your key suppliers performing? How well is your IT department functioning? How fast is the system? How easy is it to access data? How long are you waiting for issues to be resolved, and are users kept up to date with progress? How frequently is the system not available when you need it to be? How complicated is it for you to work remotely? Are you making do with work-arounds? What frustrates you about IT?

You don't have to accept work-arounds or second best. If you're investing in IT, it should be working well for you.



Do you have any single points of failure?

IT is actually one part of your business for which it can be fairly easy and cost effective to eliminate single points of failure. Whether it's the danger of having all IT knowledge residing in one place or dependence on a particular bit of kit that would bring your organisation to a standstill if it failed, you should plan to eliminate all single points of failure.

Modern servers should have built-in resilience for their core working parts; data and email should be hosted in such a way that you can still gain access if the main office is offline; phone lines should be easily diverted to mobiles if needed; your building should be served by more than one internet service provider; and you can take out insurance to provide you with access to temporary serviced offices for just a few pounds a week.

If you do have single points of failure, you should at least be aware of them and know that you have a recovery plan which can be implemented in an acceptable time-frame for your own particular needs.

A third-party IT partner can help to reduce the absolute reliance on a single in-house IT manager.

About ramsac

ramsac is an IT support and managed services provider based in Surrey. We offer a proactive 24-hour service which cuts the stress out of managing technology.

Whether it's designing a new infrastructure, migrating services to the cloud, implementing a new phone system or providing end users with really efficient and friendly IT support, ramsac manages IT on your behalf, so that you can focus on achieving your organisation's goals, safe in the knowledge that IT is secure, staff are working efficiently, and the IT investment is delivering tangible benefits to the business.

Find out more

Asking these 10 questions at least once a year, should help to safeguard your IT against the most common threats.

If you need assistance or require more robust support we would love to talk to you about your specific needs and to discuss whether you might benefit from a free IT health check.

To book an initial consultation:

Call: **01483 412 040**

Email: **info@ramsac.com**

Visit: **www.ramsac.com**

ramsac Limited
Godalming Business Centre, Woolsack Way
Godalming, Surrey
GU7 1XW

www.ramsac.com
01483 412 040

ramsac
at the heart of IT