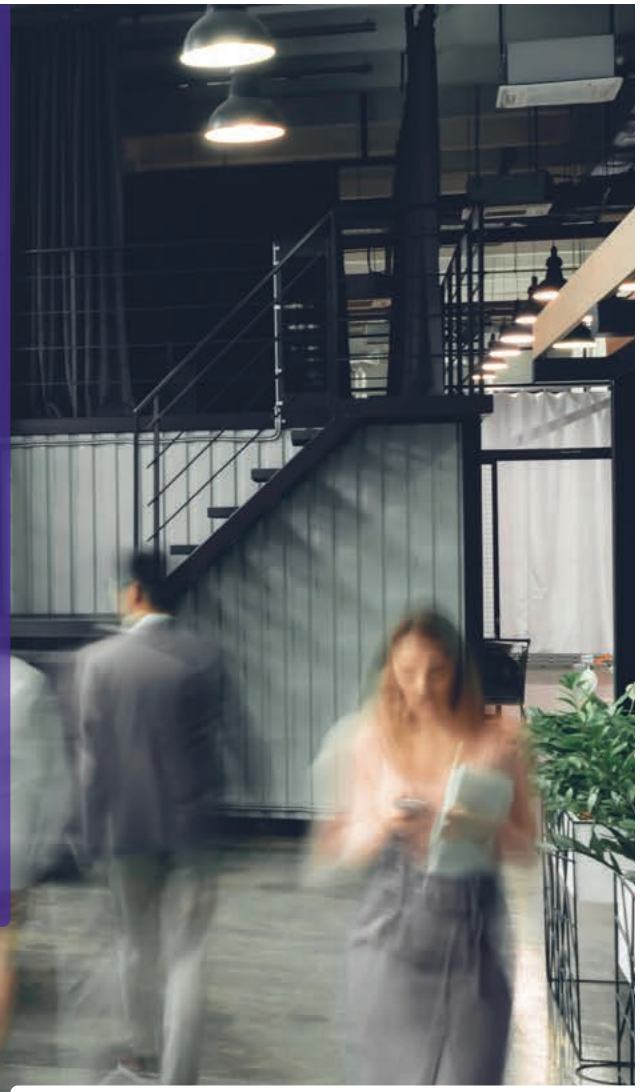
How to ensure your business enjoys World Class IT



OneCall

IT Technology and Services

Contents

About the author

Shane Ross

Originally from Tauranga, Shane has worked at OneCall since 2007, and his combination of experience in IT and logistics give him a unique take on technical challenges.

As Technical and Operations Director, Shane oversees the day-to-day running of OneCall and works with the Sales team to ensure our clients get solutions that are right for them. A skilled communicator, Shane excels at breaking down complex issues into concepts anyone can understand – 'the more challenging, the better!'

Introduction

What does 'great' look like?

This is a difficult question to answer no matter what you're talking about. But it's particularly tricky when talking IT.

All business stakeholders—the owners, the CEOs, the board members and others—understand that a great IT system is critical to modern businesses. But at the same time, these systems are now so complex that they can be incomprehensible to all but those who work in the field. There's a dichotomy here; the cleverer IT becomes, the more we need it, but the less we understand it.

So what does a Kiwi business, non-profit, charity or government organisation need to know about IT in order to construct and manage something 'great'? What is best practice? What parts make up a good IT setup? Should you manage it yourself, or seek professional help? What do you look for in such professionals?

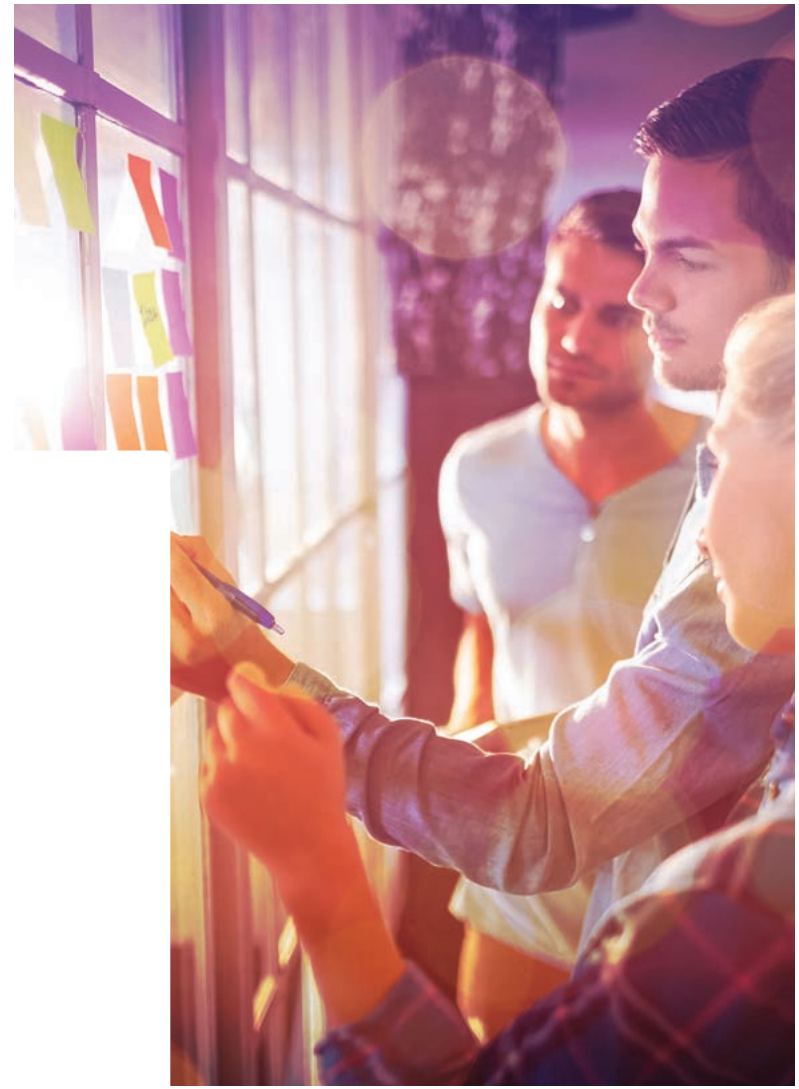
These are the questions that this eBook will look to answer.

Chapter 1

Third party providers vs internal IT teams

The first—and perhaps most important question to answer is whether you manage your IT internally, or outsource the work.

Let's take a look at when each option might be appropriate



Use a third party provider if:

1. It aligns with your strategic objective.
2. You want to reduce costs. With a third party provider you'll pay for what you use, rather than retain an IT Manager who commands an average salary of around $100k.
3. The construction and management of your IT system requires expertise across numerous areas, such as networking, security, server operating systems, cloud applications and VoIP. A third party solution provider can retain experts across a wide range of technologies—a wildly expensive thing to do in an internal team.
4. You need out of hours support. Third party providers should have sufficient staff to provide out of hours service that doesn't rely on good will at attractive rates.
5. You want to spread the responsibility. If your IT system is dependent on one or two people, what happens if they move on or get sick?

Use an internal IT team if:

1. It aligns with your strategic objective.
2. You use technology to be a differentiator in your business, and need to create and manage technology not found elsewhere.
3. An internal IT team will give you a competitive advantage.
4. You need someone on hand to respond instantly to any issues, or constantly develop technology or your IT system.
5. You are looking for ultimate control over the IT security of your organisation.
6. Your company has a large enough IT budget to retain a broad spectrum of IT skills in-house.
7. Cost is not your primary concern.

Chapter 2

The parts that make up a great IT system

2A

Cloud Computing

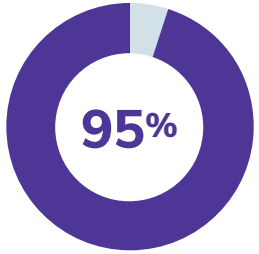
What is it

First it was the computer, then it was the internet, now it's the cloud. Cloud computing is the inescapable future, and businesses who hesitate in pulling the trigger on a cloud-driven digital transformation will find themselves lagging behind.

The value of cloud technology was laid bare at the start of 2020, as the world scrambled to make information remotely accessible to all who needed it. But even before the COVID-19 pandemic, the uptake was overwhelming—according to Forbes, by the end of 2019 an estimated 83% of enterprise workloads were in the cloud, and Cisco predicts this number to rise to 95% by 2021.

Cloud computing comes in a number of forms, most notably:

- Software as a Service (SaaS), such as Salesforce, Dropbox and Office 365.
- Platform as a Service (PaaS), such as Windows Azure, AWS Elastic Beanstalk and Google App Engine.
- Infrastructure as a Service (IaaS), such as AWS, Microsoft Azure and DigitalOcean.



Cisco predicts 95% of enterprise workloads will be in the cloud by 2021

Benefits

A move away from on-premise solutions to the cloud doesn't just strengthen your business in times of pandemics or disasters – it brings a wealth of other benefits too:

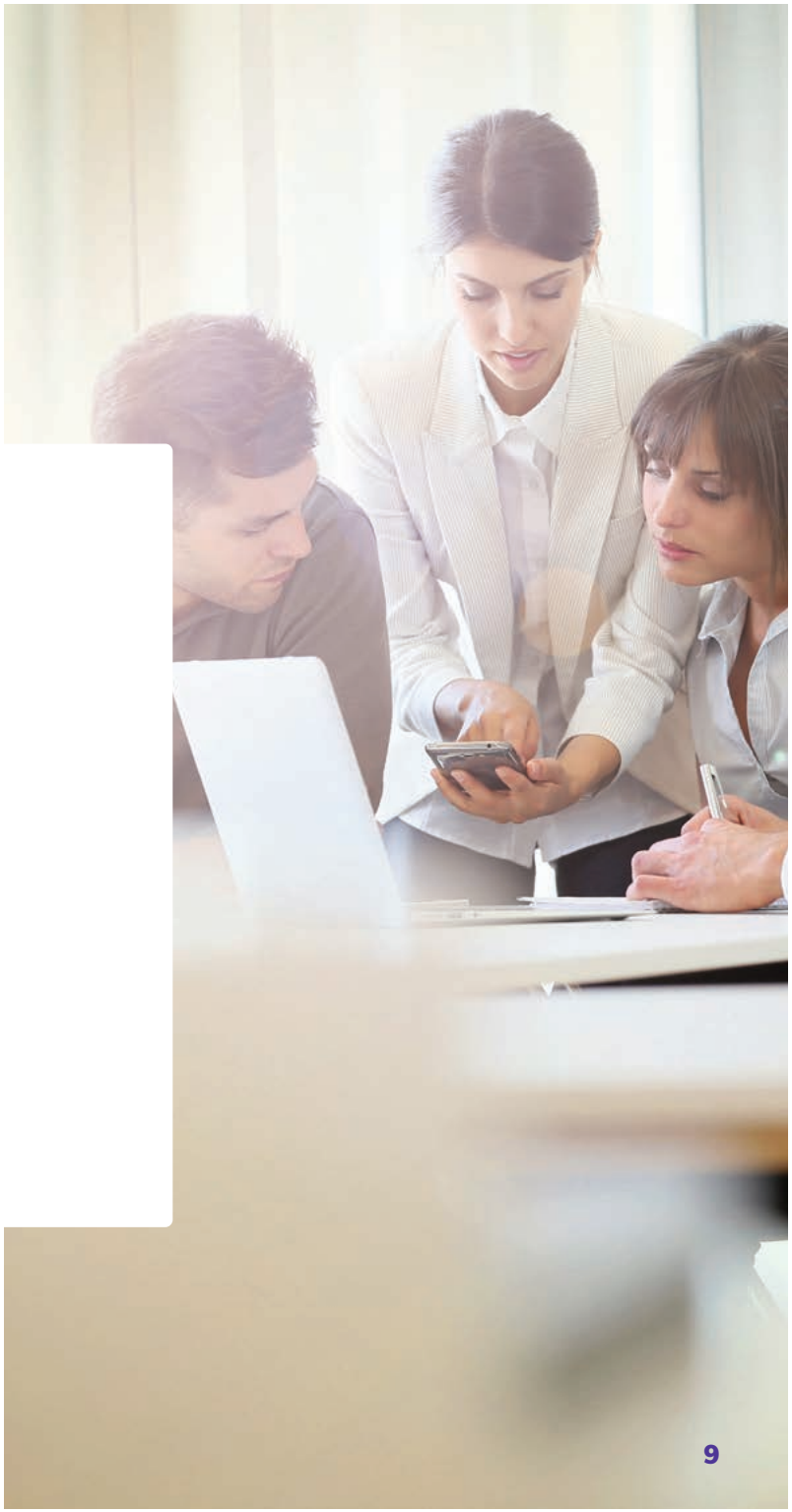
- **Remote access to information:** Currently the number one reason to conduct a digital transformation, securely storing business information in the cloud is the best way to facilitate remote work.
- **Scalability:** Instantly increase your business's storage capacity, computing power and access to software with truly scalable solutions.
- **Ultimate security:** Automatic security and software updates remove the need for ongoing maintenance and management, and keep your data and systems secure.
- **No capital expenditure:** All-inclusive subscription models allow you to pay as you go, rather than investing thousands of dollars in software and hardware. Only ever pay for what you need.
- **Remote collaboration:** Say goodbye to clunky collaboration. Live updates allow you to remotely collaborate in real-time.
- **A single source of truth:** The cloud offers total document control. You can ensure there are no conflicting files, and all team members have instant access to a single source of truth.
- **Automatic back-up:** Minimise the risk of lost data with cost-effective, up to the minute back-up and recovery solutions.

Moving to the cloud

How does an organisation begin such a momentous move?

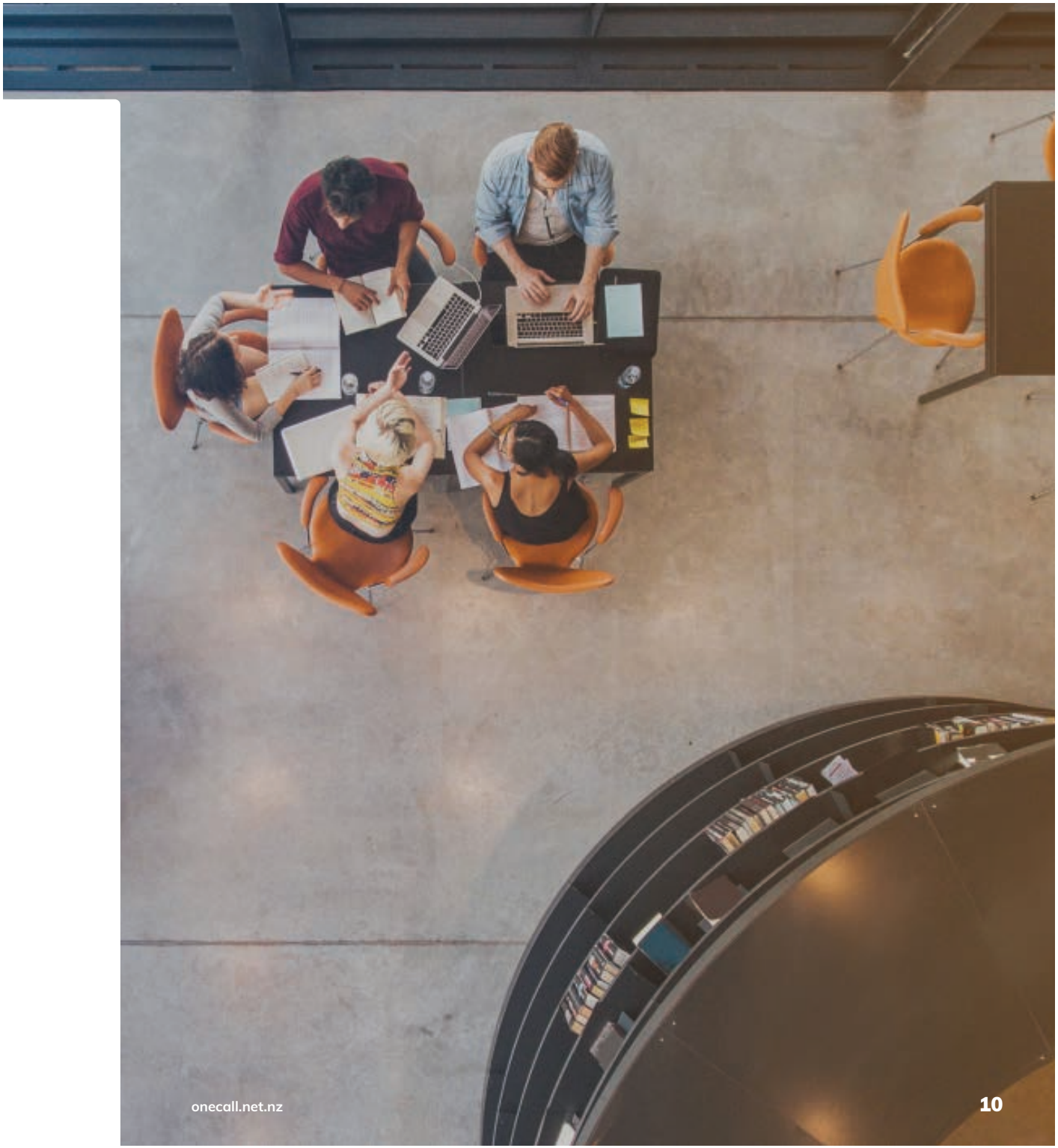
Here's a quick guide to preparing for a move to the cloud.

- **Understand your needs:** SaaS, PaaS or IaaS? What features do you need? How will you be using your solution? Do you have the necessary IT skill, or will you need some outside help?
- **Make a plan:** Decide what information and functions you're migrating, why you're migrating them, and where you're migrating them to. There may be some workloads that don't suit the cloud.
- **Conduct your digital transformation:** Once your strategy is laid out, it's time to make the switch. Use a data integration tool to move information, apps and files to the cloud, to ensure simple, secure and effective implementation.
- **Review and develop your transformation:** The process doesn't end at migration. As anyone undertaking a digital transformation will be well aware, the evolution of technology never stops. If you want to stay ahead of your competitors, you'll need to constantly review and develop your systems.



Considerations

1. Some cloud-based software vendors are 10 person companies with little experience providing enterprise grade reliability or security. Ask yourself:
    a. Where and how frequently do they backup your data? Daily, weekly, monthly?
    b. Can they restore your information in a timely manner when something goes wrong?
    c. Can this company continue to operate in a disaster?
2. Many organisations are extremely responsive during the sales process but fail when it comes to support. Where possible, test their ongoing support before you lock yourself into a contract. Ask for a trial period or speak to current customers.
3. Once you're utilising three or more cloud solutions it can become difficult to manage system access. Look for solutions offering single sign-on (SSO), as this authenticates users once through a single system, rather than having a different method for every system. SSO can be administered by an internal staff member using an agreed robust process, such as Azure AD.



2B

MFD

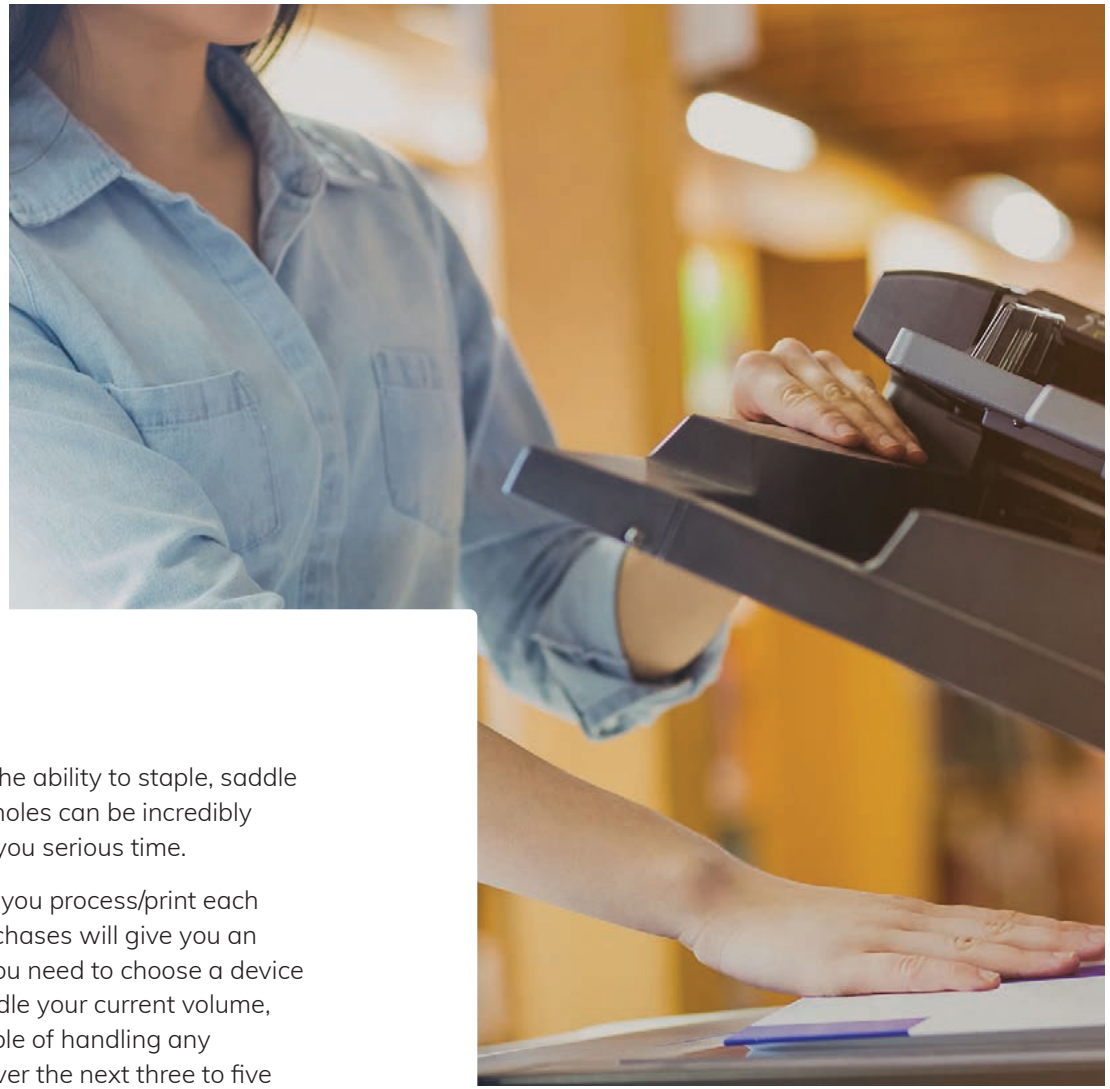
What is it

MFD stands for Multi-Function Device; other terms you might hear are Multi-Function Printer (MFP) or All-In-One (AIO). Multi-function Devices typically combine the functions of printing, scanning and photocopying. Additional features include stapling and sorting, emailing and faxing, and cloud integration with the likes of SharePoint.

Benefits

Using a single MFD offers a few advantages over having separate devices for different tasks:

- **Office space savings:** The more functions your MFD offers, the fewer stand-alone devices you need to find space for. Not having to find a separate space each for a scanner, a copier, a fax machine and a printer makes for considerable space savings in your office.
- **Cost savings:** Purchasing one machine with multiple functions provides obvious cost benefits. The cost of most MFDs is significantly less than that of buying a single machine for each of the functions offered. Maintaining one device is also more affordable than maintaining multiple machines.
- **A better user experience:** Staff must only master the use of one piece of equipment, rather than multiple devices. Many MFDs also offer additional features you may not have considered purchasing otherwise, such as faxing capability.
- **Cloud integration for greater efficiency:** An organisation may want to go paperless, but with third parties, legacy systems and long-standing processes to consider, there's always a long transition period. A cloud-ready MFD can make this transition far smoother, by integrating scans into workflows—e.g. connecting directly to SharePoint to scan and store files.



Considerations

1. If an MFD is unprotected, any sensitive information sent to the machine can be exposed. If proper security measures aren't in place, such as authorised user lists, hard drive encryption and swipe-to-print technology, it leaves you vulnerable to cyberattacks.
2. A3 or A4? If you don't have a need to handle large or odd paper sizes, an A4 device will typically take up less space and be more cost-effective than an A3 device.
3. Monochrome or colour? If you never print in colour, there's no reason to spend money on it. That said, certain colour laser MFDs can print at a quality good enough for marketing materials, which could dramatically reduce your marketing spend.
4. Special features like the ability to staple, saddle stitch, fold, or punch holes can be incredibly handy and can save you serious time.
5. How many pages do you process/print each year? Your paper purchases will give you an idea of your usage. You need to choose a device that will not only handle your current volume, but will also be capable of handling any anticipated growth over the next three to five years (keeping in mind that many organisations are going paperless.)

2C

VoIP

What is it

VoIP stands for Voice over Internet Protocol. Also called IP telephony, VoIP is a group of technologies designed to move your traditional phone systems onto the internet. Doing so can simplify the management, lower the costs, and increase the functionality of your system.

If you haven't already made the switch, now is the time, as New Zealand's copper network is slowly being switched off, meaning traditional telephony will no longer work.

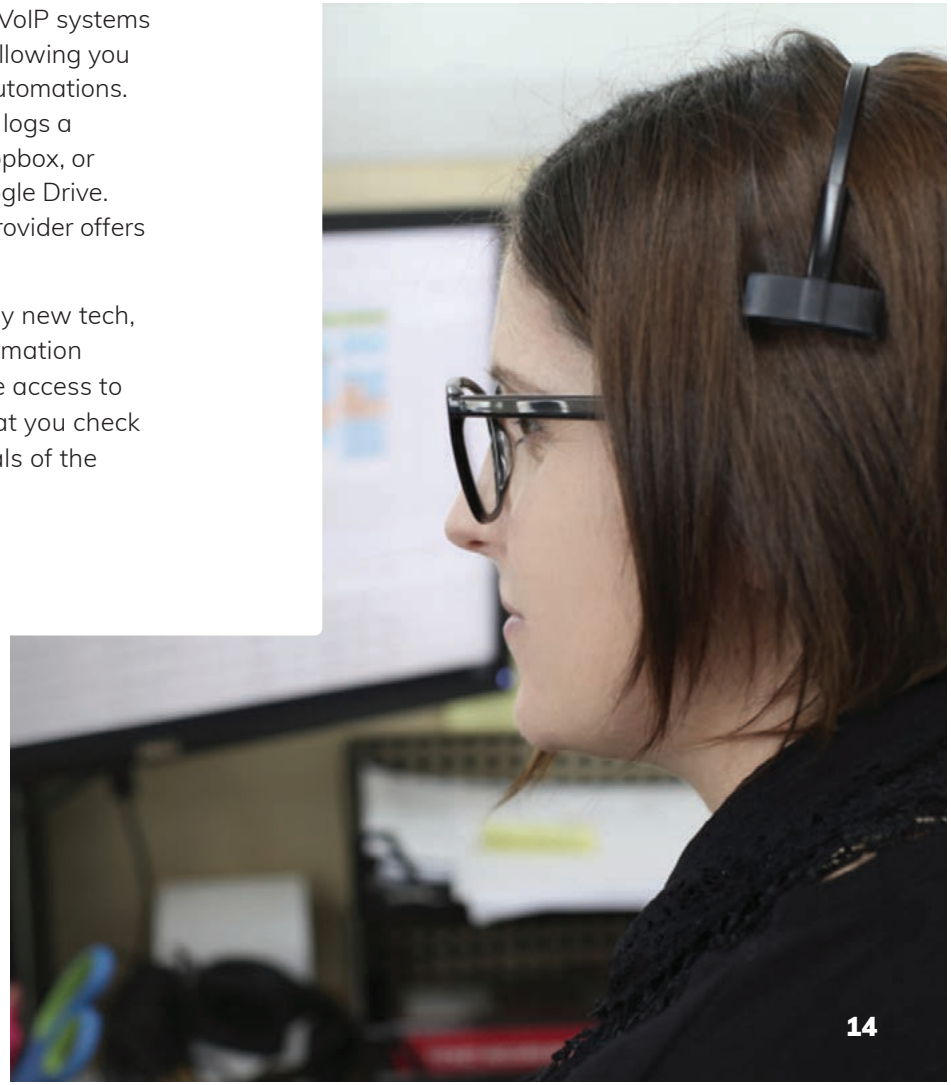
Benefits

The perks of VoIP over a traditional landline system are many and varied, including:

- **A single network:** VoIP uses your data network, removing the need to have a separate connection for your phone system.
- **Take your system anywhere:** Because a VoIP telephone system connects through the internet rather than copper wires, it can be taken anywhere. If a team member needs to work remotely, they can either take their office handset with them, or redirect calls through a softphone.
- **Ultimate scalability:** Instantly add more connections, and only pay for what you use with per-user pricing structures.
- **Clever features:** Intuitive software allows you to easily utilise and control a number of smart features, including interactive voice response, call handling, waiting and forwarding, hold music, caller ID and more.
- **Lower cost:** As long as your business has IP-enabled phones and an internet connection, you've got all the hardware you need for a VoIP system. And your choice of bundled packages or per user rates can result in dramatic savings. Based on a system of 12 users, VoIP can be less than one third of the price of an equivalent landline system.

Considerations

1. **Mobile functionality:** Remote access to your telephony is one of VoIP's most enticing features, but some providers offer better mobile apps than others. Find a provider that offers the same level of functionality on their mobile apps as they do on desktop.
2. **Call management:** If you've got a large volume of calls directed to a certain number (like a service desk) or coming in at a certain time (during peak season or first thing in the morning), call queuing becomes valuable. The best VoIP systems can intelligently distribute calls between different extensions based on availability, geography and other criteria.
3. **Third party integration:** The best VoIP systems will offer third party integrations, allowing you to create custom workflows and automations. Perhaps a call to a certain number logs a trouble ticket as a document in Dropbox, or records the call and saves it in Google Drive. Check which integrations a VoIP provider offers before locking them in.
4. **Support and security:** As with any new tech, you want to ensure that your information remains secure, and that you have access to help when you need it. It's vital that you check the support and security credentials of the VoIP provider.



2D

Video Conference Systems

What is it

The events of early 2020 showed many businesses the incredible value of video conferencing systems for the first time. Between the start of January and the start of April, Zoom's daily active user base grew from 10 million to 200 million. The age of virtual meetings was suddenly and unexpectedly thrust upon us.

There are three main types of video conferencing solutions:

- **SaaS:** This option sees a provider manage their solution through a public cloud, which an end user's hardware and software connects to. Skype, Zoom and GoToMeeting are providers of SaaS video conferencing.
- **On-premise:** All hardware and software necessary for video conferencing is kept on site. This solution is generally utilised by large organisations who want total control over their video conferencing setup, and employ dedicated staff to look after it.
- **Hybrid:** If an organisation wants the security and control of the on-premise model, but the ease and cost-efficiency of an SaaS solution, they may choose a hybrid approach, combining the best features of the two in a custom solution.

Benefits

The benefits of video conferencing, specifically SaaS solutions, were laid bare by the COVID-19 outbreak. The major perks of this tech include:

- **Greater efficiency:** Time previously spent travelling can now be better utilised. In many cases video conferencing can add hours to a worker's day.
- **Cost savings:** This greater efficiency results in serious savings, not just in better utilising an employee's time, but also for travel costs. In many cases travel across the city, country or even world can be avoided.
- **Remote working opportunities:** Video conferencing systems give your organisation the ability to offer flexible and remote working arrangements to employees, helping to attract top talent by greatly enhancing your employer brand.

Considerations

1. How compatible is the video conferencing software? Will it work with all of your in-office and mobile devices?
2. How smooth and simple is the UX? All employees should be able to use your chosen solution, and it should be simple to invite third parties to join a video call.
3. How reliable is the solution? Will it work on slow internet? Performance is paramount.
4. Is it competitively priced?
5. How simple or complex will the migration from legacy video conferencing platforms be?
6. Does the solution offer technical support?

2E

Collaboration Tools

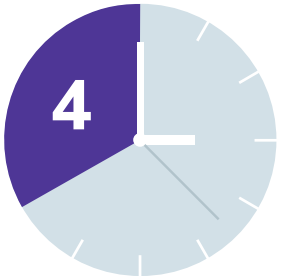
What is it

The evolution of collaboration software started slowly. In the early days it was dominated by the likes of Lotus and IBM Notes; suites that evolved from email, slowly moved to instant messaging applications, and eventually featured shared wiki pages. More recently, though, this evolution has seriously accelerated.

Collaboration tools such as Slack and Microsoft Teams offer all-in-one solutions for enterprises. They feature team workspaces, document management, instant messaging, video conferencing, and in many cases have made intra-office email obsolete.

Benefits

Like video conferencing, collaboration tools increase efficiency and reduce costs by delivering everything a team member needs to do their job right to their desk. Enjoy instant interaction and collaboration, while also visualising workflows and task management. Collaboration tools also offer team members faster access to knowledge and expert help.



4 hours/week saved by information workers through collaboration and information sharing

What do these benefits mean in real terms? According to Microsoft, their Teams collaboration tool has been shown to offer the following quantifiable benefits when compared to traditional systems:

- 4 hours/week saved by information workers through collaboration and information sharing
- 45 minutes/week saved by frontline workers through collaboration and information sharing
- 17.7% improvement in time-to-decision made by decision makers
- 18.9% reduction in meetings
- 88% of users felt “having all of our solutions in one place saves time”

Considerations

1. A collaboration tool can represent a huge change to your current internal systems and procedures. Will your organisation embrace this type of change? Are you prepared for pushback from your team?
2. But the change can't be too great. The chosen tool must integrate seamlessly with your existing application suite. It should, for example, be able to talk with your calendar and inform people if you are in a meeting.
3. This type of collaboration can be more disruptive than emails, as instant messaging creates an expectation of instant replying.
4. You will need to ensure there is a way to invite external parties safely into group chats.

2F

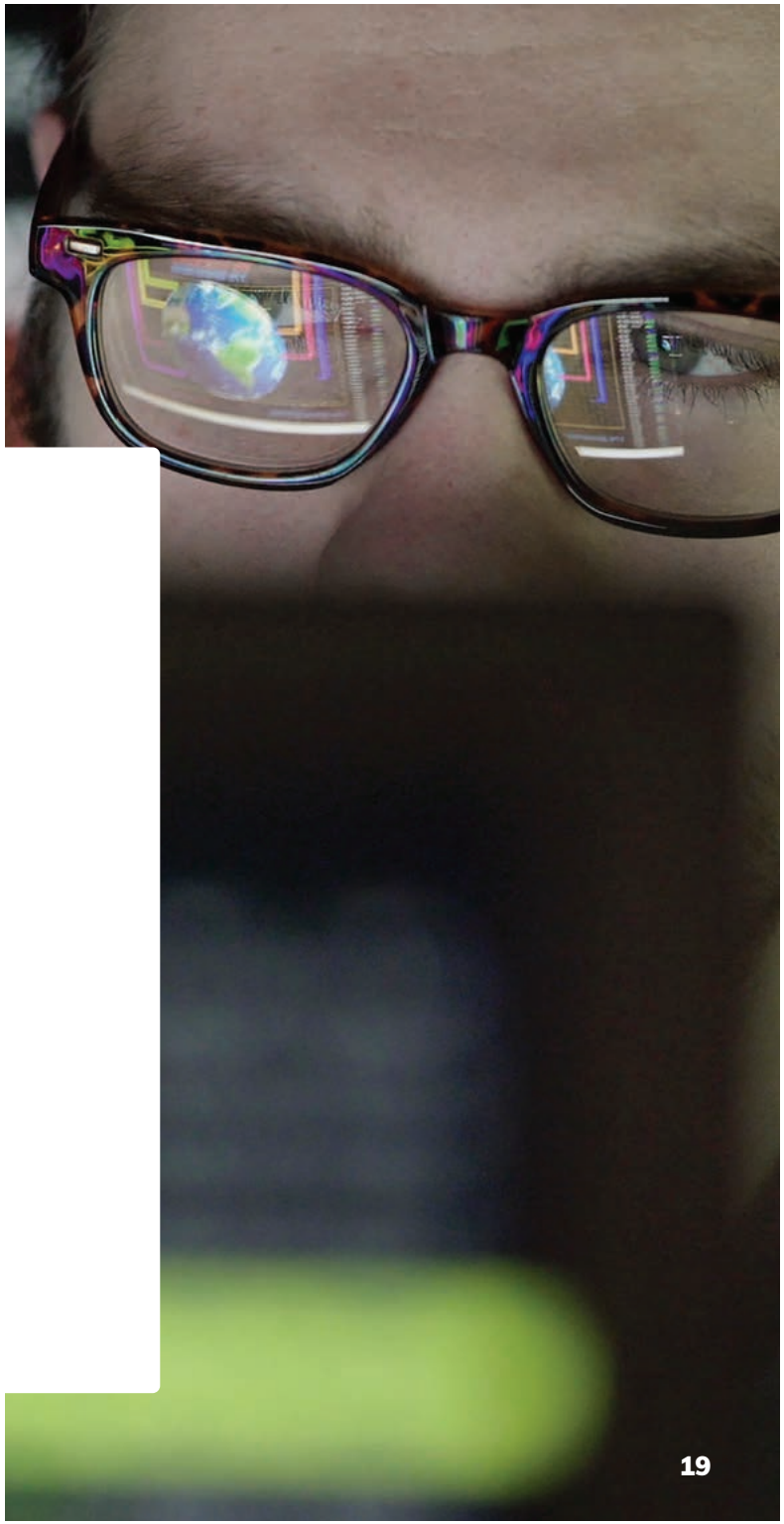
2FA / MFA

What is it

Two-factor authentication (2FA) and multi-factor authentication (MFA) are methods for identifying who an online user is by validating two or more claims from the individual. These claims can be broadly grouped into three categories:

- A thing that the user knows: A PIN, a password or the answer to a personal question.
- A thing that the user has: A known and trusted device.
- A thing that the user is: A fingerprint, voice recognition or other biometrics.

2FA/MFA seeks validation in two or more of the above categories. An email provider, for example, might check that your IP address is from a trusted device, then ask you for a password to validate something that only you would know. The greater the multiple of factors authenticated, the more secure the system.



Benefits

Where 2FA/MFA began as a luxury in the trusting world of the early internet, it's now a necessity. Aside from increasing the security and maintaining the integrity of your business systems, there are a number of other benefits that come with establishing 2FA/MFA protocols:

- **Regulatory compliance:** Many businesses in many industries are subject to regulatory compliance, and 2FA/MFA offers a way to satisfy data protection requirements.
- **Location restrictions:** Enabling employees to work remotely brings a wealth of benefits, but it also increases the risk of your devices being stolen. 2FA/MFA can help to identify when a device is being used from an unapproved location, and ask for extra validation to ensure the login attempt is genuine.
- **Simpler login processes:** Ironically, by adding more steps to the login process you can make it more user friendly. Single-factor authentication often relies on particularly long and complex passwords to guarantee security. 2FA/MFA might use more steps, but things like fingerprint scans are instant and unforgettable.

Considerations

1. Users used to single-factor authentication may see 2FA/MFA as an inconvenience and look for ways around it. It's vital that you educate your users on why you're switching, and ensure the system is user-friendly.
2. You need to strike a balance between security and usability. This will differ from organisation to organisation; a law firm will need stricter protocols than a local sports club, for example.
3. Carefully check compliance requirements, as even the strongest system is pointless if it doesn't comply with the law.
4. Have a plan in place for if/when a device is stolen. You need to ensure that no bad actor can gain access to the contents of the device, and you should be able to locate and remotely wipe it.

Chapter 3

IT service expectations

Whether you choose to employ an internal team or an external provider to construct and manage your IT system, you need to ensure that service expectations are agreed upon from the get go. Without processes and best practices being established and their use being enforced, your IT system will quickly fall into a state of disrepair.

Consider the following when developing your service expectations.

Information Security

While ultimate responsibility for information security rests with the executive, your IT team, whether internal or external, will generally take an active role in advising you on your information security strategy. They are the experts after all.

A good IT team will be transparent in how they align their information security practices with the direction given by the executive. They'll utilise recognised security frameworks, such as ISO 27001 and CIS Top 20, to form your system processes.

Information security considerations that apply to all Kiwi organisations include:

Backup, retention and restoration

Every IT system must have a comprehensive backup and retention strategy. This should not just cover all relevant business data, but should also outline a set of requirements that your cloud providers must adhere to. For example, all files backed up in the cloud must be kept encrypted, and a full backup must be completed on a regular basis (as opposed to partial or incremental backups.)

Retention is a key part of the puzzle; many organisations overlook retention, focusing on the disaster recovery aspect of backups instead. Retention is far simpler and more effective, however. Basing your data retention policy on the tax record guideline of seven years is a great place to start.

IT business continuity

Your business should already have a business continuity plan (particularly post-COVID-19), in which your IT team will play an integral part. They need to be able to outline how your key business operations will continue to run if you can't access your office, and the security protocols that surround any remote access. They also need to have strategies in place for situations in which one or more IT team members are incapacitated.

Password management

We humans are almost always the weakest part of any security framework. Our passwords are often simple, predictable or easily forgotten, compromising even the most secure of security systems. Make a password manager like LastPass or Google Password Manager or devices with built-in fingerprint readers mandatory for all users, and ensure passwords are unique and meet a good level of complexity.

Virtual Private Networks (VPNs)

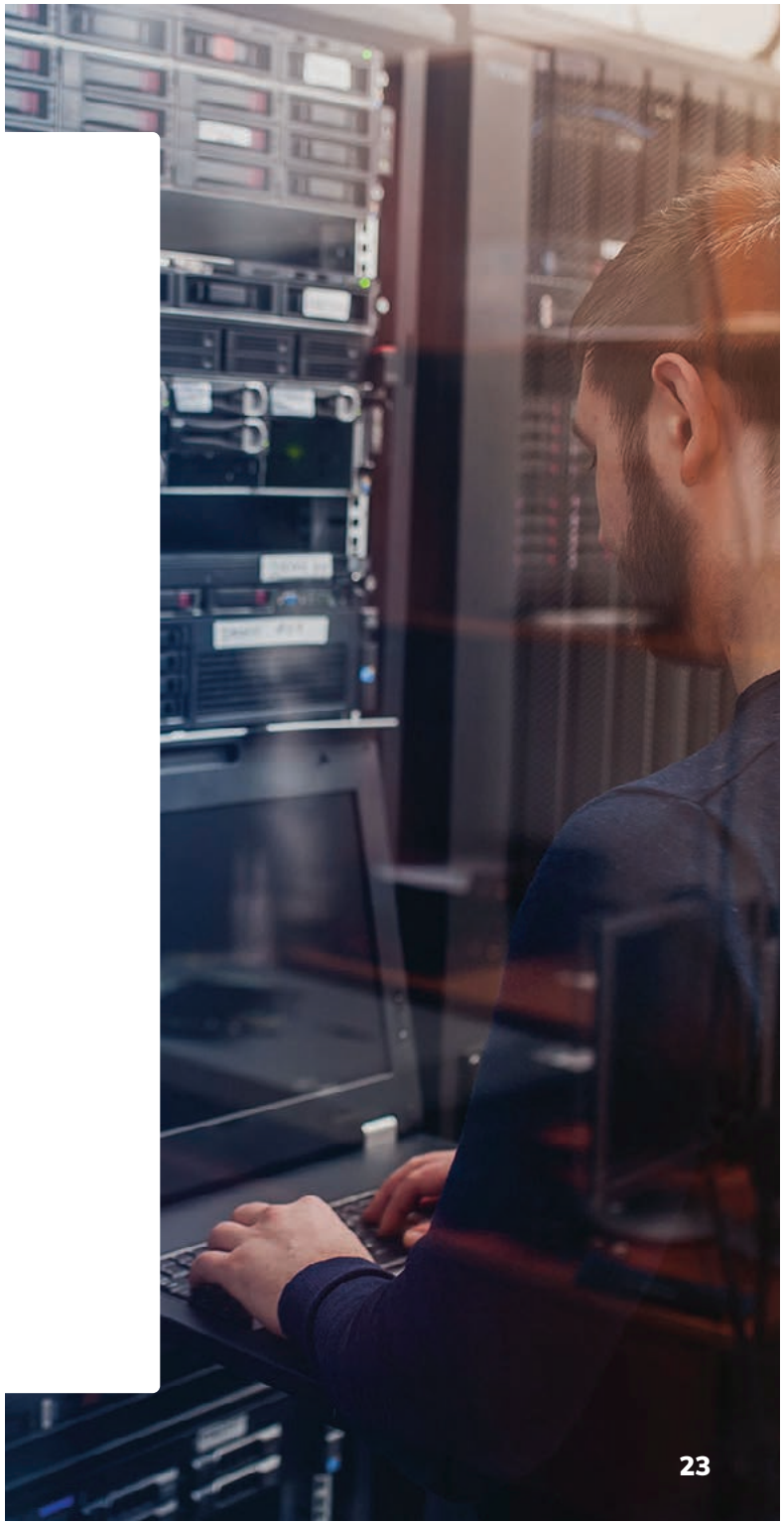
Offering encrypted traffic between on- and off-site systems, VPNs ensure that sensitive information sent between remote users stays that way.

Disaster recovery plans

While your disaster recovery plans are essentially insurance against events that you really hope don't happen, you need to ensure that these plans work if the worst occurs. Your IT team should conduct regular and thorough testing of your recovery plans, to guarantee that they'll work when you really need them to.

Response times

Internal IT teams and third party IT providers bring different levels of responsiveness to the table. Consider the following when developing your IT system, and choosing who to entrust with its management.



Remote working

Allowing remote access to your business systems means balancing accessibility with security. Your remote workers need to have access to all the systems and information they require to do their jobs, but this access can't be at the expense of the integrity of those systems. Multi-factor authentication and restricting employee access to only the areas that they truly need are two simple and effective strategies.

Responsiveness

One area that internal IT teams may outperform third party providers is in responsiveness - working under the same roof and means that an internal team is on hand to solve an emergency issue (within business hours at least.) They will be juggling multiple priorities however and may find it difficult to provide a consistent response time frame.

A good external provider will ensure that service levels are steady, by having enough staff on hand to meet demand. Ask their expected turnaround time on emergency issues and see if they're willing to outline an upper limit for response time in your contract.

System downtime

The best IT managers will minimise system downtime, bringing it as close to zero as possible. They'll keep people working by conducting compartmentalised updates and maintenance, ensuring that only small parts of the system are ever being worked on at any one time. They'll save the most disruptive maintenance for when users won't need the system, like evenings, weekends and holidays.

Prioritisation

An agreed policy must be put in place to prioritise when issues should be worked on. This policy should also outline process and timeframe expectations, to ensure best practice is being followed.

Out of office hours

A major perk of choosing a third party provider is that most will offer out of hours services. This grants you the opportunity to conduct overnight maintenance, and gives you the confidence that emergency issues will be resolved, no matter when they might occur.

Long Term Planning

Does your IT team have a growth and development plan? Does this plan align with the growth and development of your organisation as a whole?

The hardware, software, policies and procedures that you choose today can have a huge effect on your business into the future. To ensure your IT system is future-proof, consider the following when developing it:

Developing a budget

The upfront expense that can be involved in developing a future-proof IT system can be great, which can see many organisations trying to make do with what they have. But in this age of ever-accelerating technology, to stand still is to go backwards. The budget you set aside for your IT system should be seen as the investment that it is, and the question you ask yourself should be "what level of investment is required to keep our organisation at the leading edge of our industry?"

Scalability

As your organisation grows, your IT system must grow with it. So how scalable are your systems? How do you plan to support multi-office or even multinational expansion? One piece of good news is that cloud technology has made scalability exponentially simpler, with organisations able to increase their software, storage and computing capacities at the click of a button, while only ever paying for what they need.

Growth strategies

How do you intend to grow? Do you plan to take a 'business as usual' approach, and rely on steady, incremental growth? Or are you prepared to take the bull by the horns, and aim for potentially exponential growth? Your preferred method of growth will steer your level of investment in an IT system.

Avoiding complacency

One of the most common traps for IT teams is complacency. Unfortunately in the fast-paced world of tech, what was secure yesterday often isn't today, and what was market-leading last year has since been surpassed by a wealth of other offerings. A good IT team will have an insatiable appetite for innovation and will always be looking for better ways of doing things.

Conclusion

Between hardware and software, phone and video conferencing systems, digital transformation and human engagement, there are a lot of considerations to make when forming a modern IT system, and choosing who will manage it. But as IT plays an ever more important role in business, taking the time to get these things right represents an invaluable investment.

No two solutions will look the same, so getting expert advice on your organisation's unique needs is a great place to start.

Making IT work, so you can too

0800 942 002

info@onecall.net.nz

onecall.net.nz

OneCall

IT Technology and Services