

Managed IT Services RFP template

Instruction Sheet

Be sure to delete these first two pages after you have filled out the document and before you publish your public Request for Proposal.

Before you start editing the main document, fill in the following quick edit fields marked in yellow highlights. They will ensure the key information is replicated throughout the document. Don’t worry about filling them in and then deleting them – after you fill them in once, you can delete them without affecting the rest of the document. Also, don’t worry about the fact they are highlighted in yellow – that won’t be the case wherever else they show up in the document.

1. The full name of the RFP Author or Key RFP Contact’s name: [Name]
2. The position of the Key RFP contact: [Position]
3. Your organisation’s full legal name, as you want it shown in the document: [Organisation full name]
4. Your organisation’s short name, so the reader knows that you’re referring to your organisation, but not by its full formal title – this will make reading the text easier: [Org short name]
5. The phone number you can be reached on, if you want to offer it: [1300 YYY YYY or XX XXXX XXXX]. If you don’t want to offer a phone number, you will need to delete the corresponding field in [the table on this page](#_Request_for_Proposal).
6. The email address where you want respondents to send their enquiries: [Email address]

Note that if you edit any of these labels *anywhere* else in the document, you will change them *everywhere* they are used. If you want to say something different in one specific part of this RFP, it is best to delete the instance of the label and manually type in the custom text.

Editing the document

Look for red text in the document. This is a signal that you need to read an instruction or replace the text with your own content. At the end, press CTRL+A to select everything in the document, and change all the text to black at once.

How long will it take to fill it out?

When we produce an RFP from scratch, for the average organisation, it’s around 40 hours if we have all the right information to hand, and 60-120 hours if we need to discover it first. For you, if this is your first time but you have all the right information at hand, you should anticipate it will take 2-3 days to fill it in, send it for feedback to others in your organisation, and make your final corrections. Considering that you are about to embark on a new twelve- to sixty-month relationship, we would suggest it is a worthwhile investment of time.

What will be your RFP Process?

Before you fill in this document, you need to be sure of how you will approach the market, gather interested parties, evaluate and then make your final decision on your new (or retained) ICT partner.

We have written this document from the perspective of a non-governmental organisation that does not have a panel of pre-approved suppliers. If that’s you, then we have reasoned you will need to first engage with a wide pool of potential respondents, then a smaller pool of actual respondents. Then, you will shortlist three organisations before deciding on a preferred supplier with whom you will conduct final negotiations.

Depending on the complexity of your organisation though, you may wish to add more due diligence into the decision-making process, such as a site visit to the premises of your new provider or interviews with key staff members. Or indeed, you may choose to separate the Initial Planning Study phase (which is critically important no matter which company you select) from the Onboarding and ongoing Service Delivery components – to be sure of your long-term choice before you sign up to a long-term deal.

Adding those extra elements to the document is relatively easy, but if you would like a second opinion on where to locate them or how to word them, Computer One can assist.

Unsure how to make the right decision?

If this is your first time going to market, or your first time in a while, it is important to assess if you have the ability to make the right decision. If you are unsure of the amount of due diligence to apply, or how to spot the good providers from the also-rans, perhaps consider speaking with Computer One. While we normally like to throw our hat in the ring and compete for your Managed Service opportunity, we are also often used by clients as an independent advisor to review submissions or even run the entire selection process at arm’s length. In that circumstance, we do not participate in the RFP process as a potential ICT partner and that is perfectly fine with us!

Want more information?

Feel free to reach out to us to discuss any question you have regarding this document.

You can reach us on 1300 667 871, the Contact Us page on our website, or sales@computerone.com.au

This is the title page – providing you have added in the key details requested on page 1 above you can delete the previous pages now.

Once you place it, your logo will appear in the header above so there is no need to add it again in this space.

Request for Proposal RFP-202X

Managed ICT Services and Services Upgrade

This is our suggested title. Feel free to replace it as you wish.

For: **[Organisation full name]**

Prepared by: **[Name]**

Date: **Month, 202X**

COMMERCIAL-IN-CONFIDENCE

This document includes Commercial-in-Confidence information relating to [Organisation full name] which may not be disclosed to third parties for any reason unless it is related to the production of a complying response.

Contents

[Request for Proposal Process 6](#_Toc134525745)

[RFP Planned Timeline 8](#_Toc134525746)

[Organisational Summary 10](#_Toc134525747)

[About [Organisation full name] 10](#_Toc134525748)

[Current ICT Setup 12](#_Toc134525749)

[Staff, Devices, Networks and Servers - Overview 12](#_Toc134525750)

[Applications and Services - Overview 14](#_Toc134525751)

[Support Services 15](#_Toc134525752)

[Expected Service Levels 15](#_Toc134525753)

[Target Service Level Agreements (SLA’s) 16](#_Toc134525754)

[Consequences of Failed Delivery 17](#_Toc134525755)

[Server Operations Availability 17](#_Toc134525756)

[Server Maintenance 18](#_Toc134525757)

[Server Application Support 19](#_Toc134525758)

[Management of Software as a Service and Infrastructure as a Service 19](#_Toc134525759)

[Technology Strategy 20](#_Toc134525760)

[Account Management 20](#_Toc134525761)

[Information Security 20](#_Toc134525762)

[Redundancy / Backup Recovery 21](#_Toc134525763)

[Desktop Support 23](#_Toc134525764)

[Onboarding and Offboarding Users 24](#_Toc134525765)

[Network links and voice services 24](#_Toc134525766)

[Procurement and Asset Management 25](#_Toc134525767)

[Monitoring 26](#_Toc134525768)

[Support Service Delivery 26](#_Toc134525769)

[Support Procedure and Reporting 27](#_Toc134525770)

[Data Sovereignty to be assured 27](#_Toc134525771)

[Onboarding 28](#_Toc134525772)

[Managed Services Onboarding/Transition 28](#_Toc134525773)

[Sub-contracting 29](#_Toc134525774)

[ICT Remediation Activity 31](#_Toc134525775)

[Backup Service Transition: Server Cloud Backup and Disaster Recovery 32](#_Toc134525776)

[Security Audit and Remediation 32](#_Toc134525777)

[Email Migration to Exchange Online and ATP2 33](#_Toc134525778)

[Modern Device Management (MDM) to be implemented 33](#_Toc134525779)

[Licensing Remediation and Software Asset Management 34](#_Toc134525780)

[Local Area Network Remediation (head office and sites) 35](#_Toc134525781)

[Windows 11 Management Operating Environment 35](#_Toc134525782)

[Contract Terms and End of Managed Services Agreement 36](#_Toc134525783)

[The Framework for Delivery of ICT Services 37](#_Toc134525784)

[Governance 37](#_Toc134525785)

[Compliance 37](#_Toc134525786)

[Managed Services Cost Model 38](#_Toc134525787)

[MSP Response format and required information 39](#_Toc134525788)

[Proposal Evaluation Process 43](#_Toc134525789)

[Evaluation Criteria 43](#_Toc134525790)

[Thank-you 44](#_Toc134525791)

[Appendix 1. Staff, Devices, Networks and Servers - Overview 45](#_Toc134525792)

[Appendix 2. Applications and Services 48](#_Toc134525793)

As you add content to this document, the page numbers in the Table of Contents will become inaccurate. Be sure to refresh the Table of Contents as the last thing you do before publishing the document and making it available to your target audience.

## Request for Proposal Process

Please indicate your intention to respond to this RFP by email to the Primary RFP Contact listed below by the Expression of Interest Close Date and Time outlined below. In addition, please provide the contact details of the individual responsible for coordinating your RFP response.

Please then submit any clarification questions by the Question Window Close Date and Time and then, finally, ensure your proposal is delivered via email by the RFP Close Date and Time. No extensions of time will be offered.

Key Information

|  |  |
| --- | --- |
| **Request for Proposal** **(RFP)** | **Managed ICT Services and Services Upgrade** |
| **Our RFP Reference** | RFP-202x-001 |
| **Release Date**  | Date of publication |
| **Primary RFP Contact** | [Name] |
| **Expression of Interest (EOI) close date and time** | This date helps you identify potential respondents so you can include them in your responses to the questions asked by others. |
| **EOI and RFP full response email address** | Please send your expression of interest and eventual RFP response to [Email address] |
| **Phone number** | If you wish to disclose a phone number, this is the place[1300 YYY YYY or XX XXXX XXXX] |
| **Question window close date and time** | Add the date when you will cease answering questions about the RFP |
| **RFP Close Date and Time** | Close date and time for responses |
| **Head Office Location**  | Add your Head office address |
| **Service Site Locations**  | Add the details of all other locations where you will require your ICT partner to provide services |
| **Selection Process**  | Describe how you would like to handle the selection process. We have described an effective process below.1. RFP released. Expressions of Interest and Confidentiality Agreements received
2. Question window period
3. Responses received.
4. Up to three providers will be shortlisted for in-person presentations
5. A preferred provider will be contacted for further negotiations
6. Providing negotiations are acceptable to all parties, the contract will be awarded and unsuccessful providers notified of the outcome.
 |
| **Responses**  | Responses should address all the selection criteria (Refer section [MSP Response format and required information](#_MSP_Response_format)) and provide all requested information.Applications to be submitted by the closing date to: [Email address]Late responses are unlikely to be accepted. |
| **Request for Further Information**  | Requests for further information can be submitted in writing between the release date and the question closing date. See the planned timeline on the next page.We will respond as quickly as we can. Note that we anticipate receiving the same question(s) multiple times and so requests with responses will be provided anonymously to all applicants who have submitted an Expression of Interest. |

## RFP Planned Timeline

The following process and key dates are planned to deliver this Request for Proposal.

|  |  |
| --- | --- |
| **Expected Completion** | **Milestone** |
| Add the date | Expression of Interest (EOI) open, inviting identified service providers to participate in the Request for Proposal process.  |
| Add the date | Service providers to respond in writing indicating their interest and include a completed Confidentiality and Product Disclosure Agreement. EOI closes COB (5pm). |
| Add the date | [Organisation full name] to inspect EOI’s and create a list of interested parties. |
| Add the date | Service providers can put forward any questions regarding the provided information and the requested proposal in writing.Question windows closes COB (5pm). |
| Add the date | [Organisation full name] to provide anonymous written responses to relevant questions to all prospective service providers (creating a level playing field between potential respondents). |
| Add the date | Service providers to submit their final proposal to [Organisation full name] in writing to the specified email address on the Request for Proposal Process page above. Request for proposal window for submission closes COB (5pm). Late proposals are unlikely to be accepted.Note: you may be asked by one or more potential respondents to postpone the closing date to allow them to respond. Providing you have allowed sufficient time (3 weeks for simple organisations 10-500 staff, 4-5 weeks for larger or more complex organisations, you should resist the urge to allow extra time. This is enough time for organisations with sufficient resources to respond professionally and failure to meet your first deadline is a good indicator of organisations that may struggle to fulfil their service promises and deliver timely service) |
| Add the date | [Organisation full name] will evaluate and invite shortlisted service providers to present their solution and answer questions. |
| Add the date | Shortlisted service providers to present to the selection panel at an agreed time before this date. |
| Add the date | [Organisation full name] will identify and commence negotiation with the preferred service provider. |
| Add the date | Contract finalisation is expected. |
| Add the date | Initial Planning Study (IPS) to commence |
| Add the date | IPS results presented to [Organisation full name] Variations to expectation are discussed and agreed. |
| Add the date | Onboarding begins |
| Add the date | Cutover of service |
|  |  |
| NB: This is an estimated timeframe, actual activities and timeframes may be subject to change. Participation in the process is at the service provider’s own cost at all times. |

## Organisational Summary

### About [Organisation full name]

[Organisation full name] is … describe your organisation in terms of what it is, what it does, how many people are employed, who it serves, where its locations are, etc. This is not the IT description of the organisation but rather, a business overview.

Don’t forget to include: [Organisation full name] manufactures these products / provides these services…

[Organisation full name] has the following registrations/certifications… add all that are relevant. If IT has some impact on your ability to retain and build on these registrations/certifications, then that is quite relevant to the RFP document.

[Organisation full name] is committed to the health and safety of all staff, participants, families / carers, contractors and visitors. [Organisation full name] operates in accordance with [Organisation full name] policies and is compliant with the add your local workplace health and safety legislation/regulation name.

[Organisation full name] Mission and Values

If you have a mission and/or values statement for your organisation, this is where you would paste it. It will help service providers demonstrate how their values align with yours in their responses.

Strategic Vision

We have left in some guiding text here, but you may choose to replace it wholesale.

[Organisation full name]’s strategic plan includes a strategic objective of growth and we recognise that our ICT and Digital platforms are a key enabler to deliver on our organisational goals.

Our vision is to be…add in your vision statement and we will achieve this vision by 20XX.

Outcome Sought

This is where you describe the overall intent of the RFP process. You are recruiting a new ICT partner, yes, but to what end? What do you need them to do for you in summary terms? We have offered a real-life prior example below that you might want to adapt for your own purposes.

If this part has you confused over what to write, because you’re actually not quite sure what specific features you require in your new partner and what you need them to do for you apart from broadly managing your IT function better than what you currently have, we suggest splitting your RFP process into two parts and, in the first instance, finding a partner who can conduct an Initial Planning Study (IPS) and then help you write this part of the larger RFP. The IPS is an important “discovery” event that should always precede the onboarding stage of a new service provider – it helps uncover anything that will pose an issue during onboarding. But, it can also be run as a standalone project that produces the level of detail required to run a successful RFP process. Computer One can carry out an IPS for you and help write the larger RFP.

[Organisation full name] has identified a requirement to increase the maturity of its ICT environment. This includes changes to our ICT infrastructure, support and governance arrangements to meet current and future business requirements. We need to improve our ability to deliver the ICT services that support current operations and enable future business growth, while at the same time mitigating existing and unknown ICT risks.

The overall outcome sought is a partnership to develop ICT systems that will ensure seamless future scalability and cost-efficient service.

[Organisation full name] wishes to engage with a suitable Managed Service Provider (MSP) that can provide dependable Managed ICT Services for our existing infrastructure environment, including servers, workstations, desktops, mobile devices and BYOD.

A further requirement is to accelerate [Organisation full name]’s journey to flexible and scalable cloud services to meet current and future business strategic objectives.

While [Organisation full name] is flexible as to how its business requirements are met by its future Managed Services partner, it has identified several key requirements relevant to its ICT infrastructure: (Obviously, you would customise this list to your own requirements)

* Move to a more flexible, cloud-based, software-defined service and network architecture for both production and fail-over/disaster recovery.
* Transition of on-site infrastructure to Azure
* Transition of existing productivity applications to Microsoft 365 products and adoption of that platform’s capability
* Management of cybersecurity risk through reduction of attack surface and active monitoring of endpoints and server operations
* Cloud-based backup and disaster recovery capability in Microsoft Azure
* Integrated Microsoft solutions are preferred to multi-vendor solutions (e.g. utilising Microsoft Azure AD, ATP, Sentinel, Intune) – where this is feasible.
* When taking snapshots of virtual servers, application-consistent snapshots are preferable, however crash-consistent recovery may be acceptable.

[Organisation full name] also requires the MSP to provide and/or manage a full range of ICT Services. This includes:

* ITIL-based methodology to deliver ICT services that meet agreed service levels (SLAs).
* End-user support (Help Desk) including support for PCs and mobile devices.
* Management of cloud-provided ICT services (Software as a Service).
* Management of end-user devices and their security compliance status.
* Maintaining of infrastructure (including all hardware and software applications).
* Information Security Management
* Ongoing monitoring and reporting on performance and status of software, hardware, services and security vulnerabilities.

[Organisation full name] intends to develop and maintain a strong partnership and collaborate with the successful MSP. While the experience and technical competency of the Service Provider is important, [Organisation full name] also places a strong weighting on the alignment of values and culture between both organisations.

## Current ICT Setup

This section is where you describe all the features (user numbers, count of endpoints and servers and switches and software licenses, etc.) that make up the body of work you would like the service provider to manage.

### Staff, Devices, Networks and Servers - Overview

The following table provides an overview of the [Organisation full name] ICT platform.

|  |  |
| --- | --- |
| Platform Element | Details |
| Staff | Total Staff Approx: XXXApprox XX Full Time staff, XX Part Time staff, XX Casual. XX staff members work remotely.Indicate what percentage of each type of staff member needs access to a dedicated versus shared PC. Eg. If you have 100 staff, but 20 are part-time, you may only need 90 PC’s as 20 are shared (80 + 10 Full-time equivalent) |
| Server | Describe the following:How many serversWhat brand and what are the specs for each – Operating system, memory, CPU? Consolidate the information where possible – eg. If all servers are the same spec, you can just tell the reader how many you have rather than repeating the same specs XX times.Where are the servers located?Which are physical versus virtual?What is your current backup regime? |
| Data Centre locations | Where are your data centres? What brand (if public cloud) and where do you connect with them? |
| User devices | This is where you will describe the user endpoints that access your networkTypes: Desktops / Laptops / Tablets / PhonesBrandsModelsNumbersAre they company-owned or BYOD?For mobile devices (notebooks and phones) how do you control their access to organisational resources? Do you use Microsoft Endpoint Manager (Intune) or similar?How do your users access their productivity applications like Word and Excel or Adobe Creative Suite etc? Are they locally installed or accessed via cloud services?Indicate how many endpoints are active. If you plan to grow, provide an estimate of growth in Year 1. |
| WAN | Describe your wide area network. Describe the use and specs of fibre, wireless or other connection that each site uses.Who supplies your Internet services? If you have more than one contract, when do they each expire? Do you have private, dedicated links or do you go via public Internet?Are remote sites able to access Internet directly or do they get it through Head Office? |
| LAN | Describe your Local Area Networks per site. What class of network addressing do you use? What devices are connected to your LANs?What wireless access points do you use for Wi-Fi? Brand and model number will help.What security standards around connection are present in the wi-fi network? Eg. Do you have a guest network that is restricted in the services it can connect to, or can anyone who joins the network see all devices?How are edge switches and access points managed? |
| Switches/Firewalls | Describe all the switches and firewalls in use, both on-premises and cloud-based. Indicate which is which and where they are located. |
| Wi-Fi | How many access points? What brand? |
| Phones | What kind of phone system does the organisation run? What brand and model are your handsets, if you still use those? |
| Active Directory | How many domain controllers do you have? Where is it / are they located and what do they each host?How many active staff accounts are there? Note that this may be different to the number of current users on staff.How many inactive accounts? |
| Email | How do you run your email? An Exchange server? Google Mail? Something else? Where is your exchange located?What, if any, protection do you have running on your mail services? |
| Printers | How many printers do you have, what brands and models are they and where are they located?Indicate if they are owned or leased. If they are leased, are you paying for the lease through toner consumption? Do you also receive maintenance services under your current agreement?Indicate if you would like printing supply management (toners and repairs) to be part of the managed services you are seeking.If you are already under a managed service agreement for your printers, but you would like to switch, indicate when the current contract is set to expire. |
| Specialist Hardware | Such as a CCTV system or factory technology you would like your MSP to play a role in managing. |

### Applications and Services - Overview

|  |  |
| --- | --- |
| Application | Details |
| Microsoft Office 365 | Indicate how many 365-based products you have licensed and what version of 365 software they areEg. Microsoft 365 Business Premium, Business Basic, Enterprise E3, E5 etc. |
| ERP Software  | Do you use a particular piece of software to run your business, like an ERP programme? This is where you would describe it. |
| Security | Indicate the security products you use. This may be anti-malware, endpoint detection and response, mail protection, security incident and event management etc. |
| Accounting package |  |
| Anti-malware |  |
| Backup Software |  |
| Email client | Which email client do you use? |
| File Server  |  |
| IT Service Management |  |
| Network agents |  |
| HR / Payroll software |  |
| Software Asset Management system |  |
| Telephony | For those companies using a softphone application |
| Terminal Services |  |
| Miscellaneous on-premise applications | List the additional applications that are run in your environment. Eg. Document Management System, Supply chain software, specialist video editing, graphic design, video surveillance, Intranet, Custom software.Then tell the MSP whether providing services for these applications is in scope of the arrangement you are seeking, or not. Bear in mind that while an MSP *can* learn to support your entire application set, it is often much more cost-efficient to have the MSP act as a central support collation point and a liaison/interpreter between the internal application owners and external application vendors. In this scenario, the MSP acts as the manager of a resolution rather than providing it directly – it can be a lot cheaper than having the MSP’s team learn the specifics of your software.  |
| Miscellaneous Software-as-a-Service applications | Applications like Zoom video conferencing etc. Cloud-based security software or a CRM system that you want to tie into single sign-on services. |

## Support Services

This is the section where you lay out your service expectations for the new Managed Services partner. We have provided our own service definitions and expectations, which we have found to be a little higher than average.

This section spells out the scope and requirements for support services. The prospective MSP will need to demonstrate how these can be met by their proposal.

### Expected Service Levels

While the exact scope of the supplied services is up to the individual prospective MSP to propose, [Organisation full name] requires a minimum standard to which services are provided.

Services will be provided to [Organisation full name] in the Eastern Australian (Brisbane / Sydney / Melbourne) time zone. In terms of Support Services, the hours of coverage are defined as:

* Business Hours: Mon – Fri 8am – 6pm Eastern Australian.
* Extended Business Hours: Mon – Fri: 6am – 10pm, Sat/Sun 6am – 10pm.
* After hours (all other times), as well as gazetted Public Holidays.

The impact of daylight savings time will be mitigated by the MSP to ensure service provision remains within the hours of coverage specified above.

Expected Service Levels are described in relation to the priority that is assigned to a particular request for assistance. These are the categories of priority:

Priority 1: Urgent:

* Problems affecting critical systems for a large number of staff, to which there is no workaround available, or issues likely to result in substantial loss of revenue, or a significant impact on an interested party’s physical or mental health.
* Issues notified (e.g. by automated systems), which are likely to result in the above.
* Important issues affecting staff from a predefined VIP user group.
* Cybersecurity events with potential to affect the privacy of system participants and staff or that are likely to be notifiable events to the Office of the Australian Information Commissioner (OAIC).

Priority 2: Important:

* Problems affecting critical systems for individual staff with no workaround, or
* Problems affecting critical systems for a large number of staff, to which there is a workaround available, or
* Problems affecting non-critical systems for a large number of staff
* Staff priority access terminations and other urgent access restrictions.

Priority 3: Standard:

* Issues affecting non-critical systems for one or a few staff members
* Issues causing minor annoyance to a large number of staff.

Priority 4: Non-urgent:

* Requested changes to desktop, printer or server configuration.
* New user account creations.

Priority 5: Maintenance:

* Non-critical alerts and issues, which do not affect users.

Specific requests or tickets can be “prioritised” by executive staff or the Org short name inhouse ICT team based on extenuating circumstances.

While the prospective MSP may propose different priority levels and definitions, the above categorisations are used as references in the target SLAs described below.

### Target Service Level Agreements (SLA’s)

In the table below are the standard times we recommend for issue acknowledgement and resolution work commencing. Most MSP’s should be able to meet and exceed these time frames, every time.

Note: It’s important to distinguish between an acknowledgement + resolution commencement time, and full resolution time. The MSP can guarantee a response and resolution commencement time, but guaranteeing all issues are going to be resolved in a given time period is tricky because the nature of outages is almost always unique and may not reside with the MSP to resolve at all. Eg. A fibre cable being sliced on the street may result in a Priority 1 loss of internet for the whole organisation, but the ultimate responsibility for resolution is with your telecommunications provider, not with the MSP. The MSP’s job, in that situation, is to enact the Business Continuity plan, switch to a backup data source and keep you apprised of developments by the telco. The actual ticket may not be resolved for several days, and experienced MSP’s know they cannot accurately predict the resolution timeframe for this and similar scenarios.

The following response times must be guaranteed in the MSP’s SLA. If the MSP is unable to meet the requirements, alternative arrangements with the same or better outcome should be proposed:

|  |  |  |  |
| --- | --- | --- | --- |
| Priority Category | Business HoursAssigned within / Resolution commences | Extended HoursAssigned within / Resolution commences | After HoursAssigned within / Resolution commences |

|  |  |  |  |
| --- | --- | --- | --- |
| Priority 1: Urgent | 30min/30min | 1h/1h | 1h/2h |
| Priority 2: Important | 1h/1h | 2h/2h | Next business day |
| Priority 3: Standard | 4h/8h (1 business day) | 1d/1d | n/a |
| Priority 4: Non-urgent | Within 2 business days | n/a | n/a |
| Priority 5: Maintenance | Next maintenance visit | n/a | n/a |

### Consequences of Failed Delivery

The prospective MSP should also include information on any rebates relating to the non-delivery of agreed service levels in a given calendar month and explain how they are to be calculated and made available to Org short name.

### Server Operations Availability

Server operations are critically important to our work. Server operations must provide a high level of system uptime.

Here are our SLA requirements regarding server availability.

|  |  |  |
| --- | --- | --- |
| SLA | Critical Systems | Non-critical systems |
| Downtime per month during Business Hours | No more than 30 minutes (99.77% availability) | No more than 60 minutes(99.54% availability) |
| Downtime per month during extended business hours | No more than 60 minutes(99.63% availability) | No more than 90 minutes(99.44% availability) |
| Disruption events per month during extended business hours | No more than 5 scheduled or unscheduled disruptions | No more than 8 scheduled or unscheduled disruptions |
| Overall downtime per month, including after hours | No more than 7 hours(99% availability) | No more than 7 hours(99% availability) |

Please note these allowances for disruption include maximum tolerance for downtime for both scheduled and unscheduled outages.

Additional: Is there any particular time of day when uptime is an absolute must? E.g. perhaps at shift clock-on and clock-off times? Use this space underneath the table to tell your potential managed service partners when they cannot schedule planned downtime.

Note that we have opted for only moderate availability metrics – around 99% overall. More certainty around uptime can be delivered, of course, but the cost of extra uptime certainty is often not worth the expense for the average organisation. To correctly assess the decision, you will need to conduct a thorough investigation of the cost of downtime in your organisation and factor in the likelihood of disruption events given your current infrastructure, security posture and policy decisions. This investigation will determine the precise amount of downtime certainty to pursue in your RFP.

If you would like assistance to help make that determination, so you can be confident of the uptime metrics you are putting forward, please contact us on 1300 667 871.

### Server Maintenance

Server maintenance includes:

1. Management of adds, moves and changes (new accounts, printers, scanners etc).
2. Rectification of faults impacting users or systems in terms of functionality, security or performance.
3. Management of anti-malware protection, monitoring and application of updates.
4. Performance monitoring for CPU, memory, disk I/O and comparison against base-line with suggestions to [Organisation full name] if/when existing resources become stressed.
5. Application of patches and re-start (once a month, or more frequently if classified as critical by the software vendor).
6. Disaster Recovery Plan creation, maintenance and minor upgrades. (You may choose to remove this item and the next if you don’t need the MSP to manage your Disaster Recovery Plan. If you do not have a disaster recovery plan, or a business continuity plan, please contact us to talk about how to identify points of failure in your ICT systems and conduct an effective risk mitigation – ph 1300 667 871)
7. Disaster Recovery testing every six months, according to the Disaster Recovery plan, with confirmation of functionality of the failed-over system by Org short name staff.
8. Event log examination and investigation of anomalous behaviour.
9. Confirmation of server replication and image consistency, with automated alerts and managed resolution where an inconsistency is detected.
10. Setup and confirmation of daily backup.
11. Change to existing configuration, following ITIL-compliant processes, where that change is required to maintain fault-free functioning.

Out of scope: Server maintenance does not include:

1. Addition of new applications or services.
2. Hardware upgrades.
3. Repair of hardware faults – the management of repairs, however, is within scope.
4. Relocation of equipment to a new data centre.
5. Major upgrade of software (usually indicated by upgrading from version x.\* to x+1.\*).

The MSP must be capable of providing these out-of-scope services; however, they may be charged separately (rates to be advised as part of the proposal).

### Server Application Support

Here is where you need to describe the application support processes that suit your organisation. The template assumes you have your own in-house ICT team that can collaborate with your MSP and will handle escalated application support issues. If that’s not the case, you should describe the support processes that work for you or you may delete the description of the resolution steps and ask the MSP’s proposing their services to describe their suggested approach in their response documents.

Support for Server Applications will be collaboratively managed between the MSP, the Org short name Application Owners (System Admins), the ICT Team (ICT) and the third-party application supplier/service provider (Supplier). The process must look like this:

1. Org short name staff members will log any service difficulties within the MSP’s IT Service Management application (ITSM), which will be a single point of coordination and control.
2. The MSP will perform the initial investigation to ensure the server operating environment is functional and application services are up and visible on the network.
3. The MSP will ensure the user environment is working, e.g. check on operating systems health, and user-side network connectivity.
4. The MSP will trouble-shoot application identity to ensure that the user can authenticate (either as SSO, or application-level logon), or initiate password reset (following protocols) when required.
5. The MSP will trouble-shoot printer connectivity from the application, where required.
6. The MSP will escalate any issue with the application’s functionality (occurring post-login) to the nominated Org short name System Admin (the internal application owner) providing access to any information submitted by the user or collected by the MSP as part of initial trouble shooting.
7. For escalated issues, the System Admin will work with the staff member(s) to provide training, or further understand any functional issues, and work with the Supplier to identify a solution if required.
8. The MSP will support any environmental changes required to support the application and approved by the Org short name ICT team. This includes the preservation of state (snapshots) pre-change for a potential roll-back.
9. The MSP will support ICT and the Supplier in trouble-shooting any faults, or performance issues.
10. The MSP will assist in the installation of regular patches (standard change) and upgrades (planned changes).
11. The MSP will support ICT and the Supplier in the operation of a test/training environment and assisting in the scheduled restoration of data/system state (backups) to the test/training environment.

### Management of Software as a Service and Infrastructure as a Service

The previous section (Server Application Support) also applies to applications provided as a service (SaaS) by a third party. In this case, the MSP will need to work directly with the third party to ensure their cloud infrastructure is working correctly before escalating functional faults to the designated Org short name Application Owner.

For Infrastructure as a Service (IaaS), the MSP will need to assume responsibility for dealing with the infrastructure provider in the same way they would be supporting traditional on-premises hardware and infrastructure.

Where the MSP deems it beneficial to the interests of Org short name, they may choose to propose an upgrade to ICT services as SaaS/IaaS products. It is Org short name’s preference to enter a direct relationship with any SaaS or cloud service providers (such as Microsoft Azure), particularly where services cannot easily be moved between Cloud Service Providers (CSPs).

The MSP must provide management of all approved SaaS and IaaS (even when not contracted through the MSP), with direct escalations of faults to the SaaS/IaaS provider as required. SLA timers will pause when incidents are raised with the upstream cloud provider, however regular follow-ups with updates to the ICT team and affected staff member(s) are expected to ensure a timely resolution and good communications.

Where SaaS/IaaS services are integral to the provision of Managed Services (such as ITSM or monitoring tools), then the same SLAs apply as for other services and the MSP assumes full end-to-end responsibility.

### Technology Strategy

The MSP will include in its proposal the collaborative development of a 5-year technology roadmap that facilitates the delivery of strategic business initiatives across the organisation.

The MSP will work with Org short name’s IT department plus key members of the executive team to develop the strategic technology roadmap. The plan will take advantage of new and existing technologies to produce a pragmatic and effective technology roadmap that enables the organisation to achieve its vision and objectives.

### Account Management

Prospective MSP’s must offer an experienced and dedicated Account Manager, to be named in their proposal, who can function as an escalation point for urgent or VIP-related support requests.

### Information Security

In this section you will describe your information security expectations from the MSP. We have provided a typical security description that will help you determine the security credentials of potential MSP’s against the backdrop of a modern information security environment.

The MSP will provide and manage information security controls for Org short name consistent with the comprehensive control set described in Appendix A of the international standard ISO27001: Information Security Management Systems.

Controls are expected to be set, maintained and continuously improved in each of the following categories:

1. Information Security Policies
2. Human Resource Security
3. Asset Management
4. Access Control
5. Cryptography
6. Threat Intelligence / Endpoint Detection and Response
7. Physical and Environmental Security
8. Operations Security
9. Communications Security
10. System Acquisition, Development and Maintenance
11. Supplier Relationships
12. Information Security Incident Management
13. Business Continuity Management
14. Redundancies
15. Compliance

Please describe how you comply with, and can ensure Org short name will comply with, the individual security controls listed in each category of ISO27001 information security above.

In addition, please quote to produce a roadmap to meet all Essential Eight (Maturity Level 1) criteria in the next 6 months as a follow-on to the Onboarding project.

Finally, describe your prior experience at delivering user security awareness training to teach Org short name ‘s staff about current threats, terms, standards, and compliance requirements to help them avoid a security incident.

Preference will be given to MSP’s who can demonstrate current certification to ISO27001: Information Security Management.

### Redundancy / Backup Recovery

It is helpful to your prospective MSP’s if you are able to define how important your data is, and how important time is to your organisation. These are two really critical aspects of data recovery and business continuity.

Your Recovery Point Objective (RPO) is the maximum amount of data you are willing to risk losing forever in a business interruption incident, expressed as a period of time. 15 minutes, an hour, two hours, four or eight are all possible periods.

Your Recovery Time Objective (RTO) is how quickly you want to be able to resume normal operations. In other words, it is a measure of how quickly your RPO can be restored and your team can get back to work. One hour, 2, 4, 8, 24 or 48 hours are all possible RTO’s

Both objectives are determined by calculating how much money is at risk in the business every minute of the business day. Eg. 100 billable lawyers, charging an average of $350 per hour, are collectively billing $583 per minute. If your RPO is set at one hour and your RTO is also one hour, you are prepared to tolerate no more than $70,000 in lost time. Providing your disaster recovery and business continuity plan costs less than that amount, you have made a wise investment.

It is possible to accurately calculate the ideal RPO and RTO for every individual business that takes into account the cost of your operations, the realistic forgone revenue in an impact and the likelihood of one occurring, so you can put an accurate price on the likely cost of disruption per year and use it to assess your potential MSPs’ proposals.

We have nominated some better-than-normal RPO and RTO targets for your business below.

As a general rule, all technical and software components must either be set up in a redundant fashion or allow timely service restoration according to specified Recovery Point/Recovery time objectives.

Application-specific criteria will be developed over time. For reasons of simplicity, however, applications are distinguished between critical and non-critical services.

The following objectives should be met by the service provider:

* Recovery Point objective (RPO) (maximum acceptable loss of data): 1 hour for all services (24 x 7 x 365).
* Recovery Time objective (RTO) (time taken to restore services):
	+ For critical services: 1 hour during regular and extended business hours, 2 hours after hours / weekends / public holidays.
	+ For non-critical services: 4 hours during regular and extended business hours, 8 hours during after hours / weekends.
* Loss/corruption of a single server or network component: Ensure the fail-over/restoration of services can occur within RPO and RTO (potentially at reduced performance).
* In the event of primary location failure (such as a major event at the head office), all services must be able to be failed-over and be available from an alternative location, such as Microsoft Azure, within the RPO and RTO timeframes.
* All services under the control of the MSP must have a “point-in-time” recoverability, i.e. all systems must be able to be restored individually to a previous state (e.g. in case of system corruption) within RPO/RTO. The proposed system must provide at least 8 rolling recovery points per day during business hours.
* Backup must be provided for all server data with the following version rotations:
	+ Daily backup (Monday full, Tuesday – Friday incremental) - to be kept for 14 days.
	+ Weekly backups - to kept for 1 month.
	+ Monthly backups – to be kept for 12 months.
	+ Semi-Annual backups (end of calendar and financial year) – to be kept indefinitely during the service contract.

Note: If cloud backup/storage is proposed for backups, the MSP must be able to demonstrate how it is protected against corruption by malicious activity and software that might have gained full domain access.

* Should a fail-over to a disaster recovery environment be required, the fail-back must occur within a scheduled 6-hour outage window (e.g. overnight).

The following services are deemed to be critical in terms of target RTO/RPO:

* File Services
* Email services (including mobile email)
* Any underlying technologies used to provide these services (e.g. Hyper-V/ESX vSphere, Terminal Services, SQL Server etc).
* Fixed Line phone services
* Add your other critical services here.

Any other services are deemed to be non-critical.

The MSP must provide a written fail-over procedure it will follow, in time for the first Disaster Recovery test (6 months after completion of onboarding).

### Desktop Support

In this next section, you should describe your desktop operating environment and the support you expect. If you have a standard operating environment, describe the key software by brand, product name and version. You will also want to describe the devices accessing the software, eg. Desktop, laptop, tablet, phone.

We have written the next paragraph from the point of view of an organisation that does not currently have a standard operating environment.

Org short name does not have a standard operating environment (SOE) which would define hardware standards or software installations across its desktops. A standard is currently being developed and it is the intention of Org short name to introduce desktop/laptop standards in future.

Desktop support and maintenance provided by the MSP is to include the following as a minimum:

1. Break-fix response and management
2. Installation of approved software.
3. Installation of approved printer driver to access the local office printer(s).
4. Installation and maintenance of centrally managed anti-malware.
5. Management and installation of Operating system patches (Windows only).
6. Move, Adds and Changes
7. Support for the connection of mobile devices (corporate and personal) to Org short name email and apps (staff with personal mobiles are responsible for establishing their own Internet connectivity on their mobile devices).
8. Repair of faulty hardware, or management of end user hardware repairs and warranty.

If you are including printer support in this contract – i.e. you don’t have a separate contract for support from the company that sold you the printers, here is our suggested service level.

The MSP’s support for the rectification of printer/scanner/fax issues must include:

1. Rectification of print server, driver problems and user assignment issues.
2. Full management of up-stream print service vendors for fault rectification.
3. Support for the automated reporting of consumable levels from the device.
4. Monitoring of printer fault resolution and (when needed) escalation to senior management.

For hardware faults the Desktop support must include:

1. Identification of any requirements for off-site repairs.
2. Assess potential warranty entitlements.
3. Obtain approval from ICT management for repair cost (if not under warranty).
4. Inform staff of site visits by third party repairer (or provide instructions to ship faulty device if required).
5. Follow up with repairer to obtain status of repair at regular intervals.
6. Keeping users informed.

As a rule, all support should be provided remotely. However, in extenuating circumstances on-site support for desktop maintenance may be needed and should be arranged by the MSP. This applies to the following cases:

1. Rectification of any user issues that cannot be handled remotely or by trivial user interaction (such as power-cycling equipment).
2. Troubleshooting connectivity issues, operating system issues and hardware issues that cannot be resolved remotely or by swapping to spare equipment.
3. Installation of Operating Systems where such work cannot be executed remotely or prior to device shipment.

Where the prospective MSP does not have a direct local presence, they should explain what measures can be put in place to provide competent local assistance in all of Org short name’s service locations as described in the Key Information section above.

### Onboarding and Offboarding Users

The MSP must have processes in place to onboard or offboard team members in a timely and efficient manner.

### Network links and voice services

On the assumption that when you go to market you will still be under contract for your data services, we have included the following text. You should adjust it as necessary to suit your circumstances. If you would like the potential MSP’s to propose data services, you must give sufficient data about your bandwidth requirements, start and end points, contract length and communication protocol (NBN, private fibre, fixed wireless, 5G etc) to enable an accurate comparison between proposals.

The MSP may, in due course, offer to provide all or some of the required network data or fixed voice services. Currently Org short name has existing contractual obligations for data and voice services with TelcoName(s), who will continue to act as a provider of communication services (carrier).

Notwithstanding current delivery arrangements, the MSP must provide management of these services, with escalation of faults to the carrier(s) where needed. SLAs timers will pause when incidents have been raised with a carrier, however regular follow-ups are expected to ensure a timely resolution and good communication.

For new cloud, data and voice services provided by the MSP, these services must be contracted independently from the Managed Services component. Should the Master Service Agreement contract expire or be terminated for any reason, the continuation or termination of these services shall be determined separately.

SLAs for any carrier services provided by the prospective MSP will be negotiated separately.

### Procurement and Asset Management

The below text is pretty standard for asset management.

The incoming MSP must have adequate systems to manage Org short name’s assets. This includes full life cycle management such as specification, procurement, identification (labelling), deployment, audit reporting, tracking, licence compliance, data sanitisation for data-bearing devices and asset recovery services at end of life.

For hardware assets, the managed assets will include:

1. Server assets (both on-premise and IaaS). Adjust as relevant
2. Workstations (laptops and desktops), including location and current custodians (assigned staff members).
3. Mobile phones used in the corporate context, their custodians and service numbers
4. Desk phones, their users and service numbers.
5. Network equipment (switches, access points, routers and firewalls), including their locations.
6. Printers, including locations.

No separate management of monitors, keyboards, mice and consumables is needed.

The management of Software Assets (both “perpetual” and “subscription-based”) should include the following:

1. Current licensing entitlement for all key software (such as Microsoft Office, Line-of-Business applications).
2. Information on licensor support and maintenance arrangements / expiry.
3. Software assignments and installations to specific hardware or staff.
4. Information on installed versions (to identify and manage vulnerabilities).

It is understood that automated tools may not be able to generate all relevant information, such as the exact physical location or current custodian of an asset. In these instances, the MSP must provide a means for Org short name to efficiently provide such information as part of onboarding new staff.

The MSP must also provide a process that Org short name can integrate into its HR operations to ensure devices allocated to past staff members are reallocated to new members with the appropriate update to asset management registers.

The MSP should also manage any other assets, such as certificates for internal and public services.

Information for all assets should include relevant details, such as vendor, model, subscription/service expiry, software versions, support arrangements, location (where appropriate), assignments (to users, hardware or sites) and important technical details (for example, IP addresses), including last known configuration.

Ideally, any dependencies of the assets should also be mapped and linked to services.

Access to the Asset Management tool(s) shall be provided to Org short name ICT staff at least in read mode, however some level of editing access would be preferred, with logging of user name recorded against changes in the tool.

### Monitoring

Add or delete from these monitoring suggestions as appropriate for your organisation.

The following minimum monitoring must be in place and automatically alert the MSP (and for critical failures, Org short name ICT staff) to problems in the following areas:

1. All physical and virtual equipment, such as server, storage, routers, firewalls and core switches.
2. The availability of remote logon facility to Terminal Services.
3. Network connectivity of primary and secondary server locations.
4. Network connectivity of sites within the WAN and remote locations.
5. Replication between primary and secondary site.
6. Successful completion of scheduled backups.
7. IaaS, SaaS and public web sites. While these services are hosted externally, they will require monitoring and any technical faults managed by the suppliers.
8. Continuous application vulnerability monitoring, with alerts provided to Org short name ICT staff.

### Support Service Delivery

In this section we describe what your expectations of general service provision should be. Be upfront and clear with the service standards you expect and allow your potential managed service partner to ensure their proposal has the right amount of resources allocated to it. You will get better service over the long term because your partner won’t be locked into delivering service against expectations they misinterpreted – this is often the cause of a relationship breakdown with your MSP that forces a change of provider and unnecessary costs.

You will notice the last point below relates to the MSP being able to demonstrate how it can provide services that aren’t just about “keeping the lights on”, as they say. Your Managed Service partner should expect (and be able to) play a role in developing and executing corporate strategy, to support your various departments to develop a long-term competitive edge. This is a key element where you will see a higher return on your investment in ICT when you use a “transformational” partner focused on more than simple service level compliance.

Support services provided by the MSP’s Help Desk staff must be delivered with exceptional customer service. The MSP shall be able to demonstrate patience and empathy working with staff of varying levels of ICT literacy. This must also be assured for any arrangements involving third parties contracted by the MSP.

The MSP must allocate an Account Manager, accessible to Org short name’s delegated contact and arrange a formalised monthly account management meeting.

The MSP shall also provide a weekly Operations and Change meeting between its nominated technical lead(s) and Org short name’s ICT department. The meeting may include third-party suppliers, when required.

The MSP must be able to demonstrate what other services it can provide in the facilitation of Org short name’s strategic business objectives.

### Support Procedure and Reporting

The prospective MSP must implement a fully integrated ITIL-based support and trouble ticketing process, allowing submissions via email, telephone and web.

The prospective MSP must follow appropriate procedures and ensure all tickets are managed through an industry standard ICT Service Management system (ITMS) and adequately categorised and prioritised in accordance with well-defined standards.

Designated Org short name staff must have access to all outstanding and completed tickets, at all times, through the ITSM client portal and should be able to:

1. Create new tickets on behalf of other staff.
2. Add comments to tickets.
3. Resolve ticket (but not close).
4. Escalate priority of tickets.

An electronic monthly report must be generated and supplied to Org short name showing:

1. Any support request that has been worked on.
2. Patch Level and compliance of all endpoints and servers.
3. Anti-malware Protection Levels.
4. Software licensing compliance.
5. Availability history for all key infrastructure (servers, networks to all premises).
6. Application availability and responsiveness history (Http/Https requests only).
7. Capacity assessment to identify bottlenecks (networks, CPU, memory, disk space, disk I/O).
8. Other general “network and server health” parameters.
9. Staff satisfaction with the MSP’s support (Net Promoter Score of +70 is preferred). The Net Promoter Score algorithm is low-touch for your users and it is the global standard for customer satisfaction measurement and comparison. Scores are represented as a single number on a scale from -100 to +100. Scores above +70 are regarded as world-class because they are so hard to achieve and consistently maintain. Computer One’s rolling 30-day average NPS is almost always above +70.

The electronic report must be presented for discussion in an on-site or remote video conversation each month between the key contact of Org short name and the MSP’s account and technical staff members.

### Data Sovereignty to be assured

All data and records that are generated as part of the engagement will be owned by [Organisation full name] and may be requested at any time and will be provided or retrievable at the end of the engagement.

Without written permission otherwise, all data at rest must remain within the sovereign borders of Australia.

This includes (but is not limited to):

* Backups taken off-site during the contract period.
* All tickets for incidents, request and change records.
* Configuration data.
* Asset data (both hardware and software).
* Knowledge articles transferred to, or created by: [Organisation full name], the MSP, or any third parties in connection with the managed service relationship with [Organisation full name].

At the end of the engagement, all data transferred to [Organisation full name] must be structured and readable with common tools, such as Excel, Access or SQL Server (database backup).

## Onboarding

The successful provider will present an overall solution that includes:

* The onboarding of ICT Managed Services, including managing the change, and the rolling out of the provider’s management tools.
* An approach to each suggested remediation Work Package (Projects) outlined within the next section.

### Managed Services Onboarding/Transition

The MSP will be responsible for all aspects of the successful migration to the future ICT environment:

* The MSP must provide a service migration plan as part of the proposal.
* As part of that migration plan, the MSP must advise how the migration will proceed, and what disruptions to the operations are likely to be experienced.
* The MSP will need to identify and scope any required involvement from Org short name and other parties.
* The MSP must also advise how risk is kept to a minimum and what “roll-back” provisions will be made, if components of the service migration process fail.
* The MSP must provide full project management of the services migration.
* Any work will need to be performed in such a way that it does not significantly impact staff during business hours. Some migration work may need to be done after hours.
* Setting up of monitoring and alerting.
* The MSP will assume responsibility for the completion of any work required (either by the MSP or other third parties) to implement ICT hardware, software and new services.

In this scenario, the RFP assumes that you’re not going to be changing data providers at the same time as MSP. If you are, then you will need to add an extra dot point to the list above. If not, then the next paragraph will suffice.

The transition of network and communication (voice/data) services is not part of the initial scope, however the MSP needs to define any additional data service requirements (e.g. for data replication) as part of the onboarding.

The MSP must also advise how the interaction with carrier (and other providers) will be managed.

It is the preference that all Org short name support requests are channelled through a single point of contact provided by the MSP from the commencement of onboarding. This includes:

* Full management of all network and voice-related services, even where the services are still provided by the former MSP who will continue to act as the carrier. This includes:
	+ Establish escalation processes needing to be in-place when the carrier is not meeting SLAs.
	+ Process should ensure that users only ever interact with the MSP, and do not need to deal with the carrier directly.
* Full management of printer issues.
	+ Establish escalation process to Org short name ICT team when needed.
* Warranty and repair management for server and desktop hardware:
	+ Establish escalation process to Org short name ICT team when needed.
* Application Support Onboarding. The successful MSP needs to support all applications in the following ways:
	+ Create suitable catalogue items for logging faults, support requests and changes.
	+ Define a process to manage application support as outlined in the [Application Support section](#_Server_Application_Support).
	+ Establish a relationship with third-party suppliers to collaboratively support the resolution of faults, for installation of application patches or upgrades and the management of change.

## Sub-contracting

You may or may not wish to deal with an MSP that sub-contracts part of its services to be delivered by a third party. The typical concern is that without a direct relationship with a service provider, your organisation may not receive services to the same standard as from a primary contractor. While Computer One rarely subcontracts services, there are times when it makes sense to do so because a sub-contractor is a specialist in its field or can offer services in a location that our own resources can’t reach in a timely and effective way. In these circumstances Computer One (as with most MSP’s) remains the sole point of contact and takes responsibility for service delivery, regardless of whether it is directly or indirectly delivered. So, the concern is typically more than the reality. Regardless, we have provided two alternate approaches below. Select the one you prefer and delete the other.

While it is preferable that most services are provided by the MSP themselves, this may not always be the most effective way to deliver a service.

Where the MSP anticipates the involvement of third parties for certain parts of its service delivery, it should clearly state the scope of delegated services, name the sub-contractor(s) providing the service(s) and provide the CV’s of key service delivery team members.

OR

Org short name wishes to engage with MSP’s that can deliver the totality of services it requires from in-house resources. To that end, sub-contracting is not permitted except by written authorisation in rare circumstances. Excessive sub-contracting, as judged exclusively by Org short name, constitutes reasonable grounds for termination of the relationship.

## ICT Remediation Activity

This section is where you can describe all the projects, compliance upgrades and management tasks you already know your new (or retained) MSP will have to perform once appointed to the role. This list is typically the product of an Initial Planning Study, or IPS. It’s a good idea to have it in your RFP because it means the incoming MSP can be confident they understand the full task at hand rather than engaging in the onboarding process and discovering gaps that will set back their work by weeks or months.

If you do not have a full list of the remediation items, consider engaging a provider to conduct an IPS as a standalone project before engaging in the full RFP for managed services. If you end up selecting a different partner for your long-term managed service contract, your new MSP will still need to undertake an orientation in your organisation, but they will have the luxury of confirming the findings of the IPS rather than engaging in ground-up research all over again. You should also anticipate the onboarding cost to be less to account for the fact the whole IPS does not have to be carried out a second time.

We have added some common examples of remediation projects below, but you should adjust to suit your own organisation’s circumstances.

A range of remediation activity will be required to allow for future growth, reduce current ICT risk and underpin the resilience of critical ICT services.

The following remediation work packages will also assist the prospective MSP to meet the required service levels and success criteria outlined in the previous sections.

While details of the Remediation activity will need to be fully scoped, Org short name would like to understand the approach for each suggested Work Package, including the following information:

* Approach and brief draft architecture for the proposed packages.
* Hardware and/or software or services requirements, and the estimated cost for Org short name, both CAPEX and OPEX.
* Chargeable work performed by the MSP, including for discussion, design, planning, configuration, deployment, testing, support onboarding and project management for the proposed solution.
* Estimated duration for the implementation of a particular work package.
* The MSP will need to identify and scope any required involvement from Org short name, including for requirements gathering, solution sign-off and user acceptance testing (UAT).
* Explain how migration or service implementation will be performed in such a way that it does not significantly impact staff.
* Possibility for re-use of existing Org short name hardware, such as server hardware and network components.

It is anticipated that the incoming service provider will request to relax some service levels while the remediation activity is undertaken. The MSP must be specific in explaining which service levels will be affected, by how much and for how long.

The service provider should also feel free to add any additional remediation activity that they see as essential for the provision of the service, based on the required service levels and information architecture described in previous sections.

### Backup Service Transition: Server Cloud Backup and Disaster Recovery

Org short name will be transforming from an on-premises backup solution to cloud. Org short name prefers to use Azure IaaS components for both the backup and the operation of a secondary data centre. We will look to the preferred MSP to design and implement an Azure solution.

The design and implementation of a scalable Azure IaaS architecture must include:

* Backup of all business data to cloud in a secure environment.
* Setting up of Azure virtual networks for restored servers.
* Server restoration along defined RTO and RPO timeframes (preference for critical services).
* Capability of sand-boxed testing for the restoration of current on-prem servers hosting critical applications.
* Access from Org short name’s private IP network (VPN access or Azure Express Route) – to provide access in the event of fail-over.
* Secure Access via public Internet to a restored Terminal Server farm (including multi-factor authentication.
* Ability to transition back to on-premises production servers at the end of a disaster with minimal disruption.

The design and implementation of the backup and recovery environment should allow Org short name to ultimately transition the cloud IaaS environment to act as the primary production environment and decommission the physical server infrastructure at Head Office.

### Security Audit and Remediation

A review of the security-related components in the Org short name environment has identified several improvements that will strengthen our security posture.

Planned remediation activity should include:

* Clean-up of unused Active Directory user and computer accounts against logon activity, current staff directory and a workstation inventory / asset management system.
* Removal of local administrator account – unless this is specifically required by the role or staff situation, in which case a secondary admin account should be utilised. This should include the implementation of “break-glass” local admin accounts to assist users when needed (e.g. LAPS).
* Restriction of administrative rights to the Windows Domain for non-ICT staff, with introduction of secondary admin accounts where needed.
* Implementation of in-path web traffic scanning and reputational web filter solutions (e.g. DNS-based) to reduce the impact of risky user behaviour.
* Log scanning (e.g. for Active Directory and Office 365 logons) to identify patterns of malicious behaviour.

In the future the following aspects should be examined. In their response, the MSP is invited to demonstrate their experience and competence with:

* Application control / whitelisting to allow only known applications to be executed.
* Data-loss prevention technologies

As part of onboarding, the prospective MSP should examine the current systems for weaknesses not remedied by the suggested activities and plan additional remediation.

### Modern Device Management (MDM) to be implemented

Org short name’s current MDM implementation lacks critical features such as the identification of service numbers, users and assets.

It is, therefore, necessary to re-establish a modern device management platform, both for corporate mobile devices and select personal mobile devices used to access sensitive data.

The following requirements should be met by the implementation of the MDM. Prospective suppliers should demonstrate their experience in:

* Support for Android and iOS platform.
* Detection of compromised devices (e.g. rooted or insecure OS versions).
* Enforcing of passcode or biometric access, with a device wipe on 10th failed attempt.
* Automated deployment of critical applications including configuration.
* Network configuration deployment (such as Org short name Wi-Fi networks).
* Configuration of staff email access on mobile devices.
* Configurable blacklisting of applications which could compromise data security.
* Remote device lock and selective data wipe of Org short name data.

The prospective supplier should demonstrate their experience with implementing and maintaining Modern Device Management in organisations similar to Org short name.

### Licensing Remediation and Software Asset Management

For Org short name, licensing compliance is important and should be achieved quickly.

The successful MSP should demonstrate how they will meet the following criteria when implementing license management:

* Have a strong understanding of and be able to leverage the licensing discounts available.
* Analyse current licensing position on all “paid” applications, including Microsoft software stack products.
* Suggest remediation measures where needed, including options for direct or Cloud Service Provider (CSP) subscriptions and/or purchasing and support and maintenance options.
* Work with Org short name to establish a Software Asset Management system to track entitlements, current licensing assignments/installs, and software versions.
* Establish a process to track vulnerabilities in applications to enable a proactive response when needed.
* Work with Org short name to establish approval and purchasing processes for new software licenses. This will include SaaS licensing.

The prospective supplier should demonstrate past experience in Licensing and Software Asset Management in organisations similar to Org short name in their proposal.

### Local Area Network Remediation (head office and sites)

There is currently no segregation of network traffic between servers, wired workstations, wireless corporate workstations, guests and mobiles. The single class C network segment at Org short name’s Head Office relies on a single DHCP server. Some of the equipment is VLAN capable.

The following remediation work is planned:

* Design an overall architecture of Org short name’s networks with an assigned IP address scheme for all sites / purposes and unified VLAN assignments for corporate, voice, servers etc across all premises.
* Implementation of network ACLs to segregate network traffic and protect servers from threats such as compromised workstations.
* Mapping of SSIDs to specific VLANs, utilising 802.1x authentication against Active Directory.
* Resilience for DHCP and DNS services to withstand single failure.
* Integration of local network design into SDWAN architecture.

Prospective MSPs are required to demonstrate competence in handling such a project.

### Windows 11 Management Operating Environment

This version of the RFQ template was written when Windows 11 was the newest standard. Feel free to adapt as editions change.

The current deployment of the Windows Operating system relies on the manufacturer’s pre-installed image or a manual OS installation, with subsequent application deployment.

Org short name wishes to deploy Windows 11 and most desktop applications in an automated and standardised manner, satisfying the following requirements:

* Automated deployment of Windows 11 for all supported hardware.
* Automated joining of corporate desktops/laptops to Active Directory Domain.
* Automated deployment of all standard tools, including A/V and remote management tools.
* Automated deployment of applications – to be centrally managed.
* On-prem or cloud repository for operating system and applications.
* Transition of redirected user folders to OneDrive protected known folders.
* Use of Intune and Microsoft Defender / ATP is highly preferred.

Prospective MSP are asked to demonstrate recent successful examples of configuring automatic deployment of Windows and associated productivity software.

## Contract Terms and End of Managed Services Agreement

We have suggested a contract period of 36 months. 12-month engagements, although they may seem attractive to your organisation because they offer flexibility, are not actually all that good for the MSP as they don’t offer enough time for your partner to bed down and improve upon processes to the point where they achieve sufficient profitability. 36 months, on the other hand, is long enough for the anticipated efficiency to manifest and be passed on to you in the form of a shorter and shorter problem resolution times and/or decreased incidence of certain ticket types.

Org short name will offer the successful MSP a 36-month contract to provide managed services; however, the contract must contain a no-penalty exit clause, allowing either party to unconditionally terminate the contract with a 3-month notice period.

The successful MSP will be subject to periodic management and performance reviews assessed against the service standards agreed in the Service Level Agreement.

Where network links are provided on a fixed-term contract, they must remain usable whether Managed Services are provided by the MSP or a competitor. That is, the service agreement must allow for the continued effective provision of data links beyond the termination of the Managed Services Agreement (MSA).

Some SaaS/IaaS services may be integral to the provision of Managed Services (such as the support ticketing system, endpoint management systems or monitoring/alerting). These services must be able to be ceased without penalty with the conclusion or termination of the Managed Service agreement (with a data export provided to Org short name, as previously stipulated).

Where SaaS or IaaS services are proposed and contracted separately to the MSA on a fixed-term contract, effective use of these services must be possible when Managed Services have been terminated with the MSP and the same services are provided through a competitor. The MSP will be required to demonstrate how their proposal complies with this element.

If and when the Managed Services Agreement is terminated, the MSP must cooperate with the new, incoming Managed Service Provider and/or inhouse ICT team. Labour cost directly associated with the handover may be charged at agreed labour rates, however no cost must be charged for the following components:

1. Export and handover of Org short name’s data
2. Wiping of Org short name’s data from any data storage facility managed exclusively by the MSP. Blancco Drive Eraser and File Eraser records confirming sanitisation of data will be provided by the MSP and the associated Blancco licensing may be oncharged at cost. This is an important component of the agreement you are about to enter into – you don’t want your data to be accessible by any unauthorised party and you need to be sure that any data you do not control directly has been sanitised, such as when your MSP has provided a private cloud option.
3. Removal of any data and accounts relating to Org short name from the MSP’s internal systems (such as the ITSM or a knowledge base).
4. Tear-down of any remote access or monitoring facilities, including VPN connections.
5. Uninstallation of any software components deployed to Org short name’s hardware.

The MSP should include a project fee for the actions required in the event of termination with their proposal.

The MSP should also include a copy of their Master Service Agreement or similarly-themed contract.

## The Framework for Delivery of ICT Services

As part of the RFP response the prospective MSP must provide evidence for how it will effectively deliver its ICT Service. This includes describing its process for managing and supporting:

* High priority Incidents
* General Support Requests
* Change Management.

While strict adherence to all components of ITIL methodology is not required, the prospective MSP needs to demonstrate how their approach is aligned with ITIL methodology.

### Governance

The proposed service must include collaboration from time-to-time between the MSP and Org short name to develop customised ICT policies, to strengthen the governance position of the organisation. Org short name’s ICT department will take primary responsibility for the development of any such policies, with the MSP providing input and oversight during development.

### Compliance

It is important for Org short name to establish good working processes and achieve compliance in the following areas. The Managed Service Provider should explain how its processes will help achieve:

* Software licensing compliance – ensuring that all software and services are correctly licensed in accordance with the software vendor’s licensing terms, and ensuring compliance is maintained when changes to staffing and infrastructure are made.
* Data privacy compliance in accordance with the Australian Privacy Act 1988.
* Maintaining defined, repeatable processes for on-boarding and off-boarding of staff, and any changes in functional roles.
* Robust processes for granting staff access to confidential or sensitive applications or data.
* Protection of Org short name’s data in transit and at rest when held on Org short name’s infrastructure (including end-user devices), IaaS, SaaS or the MSP’s storage facilities.
* Compliance with data retention laws for financial data, but also for data concerning Org short name’s staff and participants.

Compliance is a joint responsibility between Org short name, the MSP and any third-party application vendors, with varying degrees of responsibility between parties.

Org short name would like the prospective Service Provider to present a coherent concept explaining how they will achieve and maintain compliance in areas directly under the MSP’s control, and how they will collaborate and contribute in areas of joint responsibility.

### Managed Services Cost Model

It is important to understand the MSP’s cost model. If you understand how they price their services, then when the scope of service that you require changes at some point in the future, you will be able to determine the impact on your required investment.

Org short name is seeking to partner with the incoming MSP to support business growth and innovation beyond the incremental improvement of the current ICT environment. As a result, it is likely that services provided will need to adapt at times to changing scope and circumstances.

Org short name understands that changes in the scope of service provision will entail a changing investment in IT. As part of having an open and transparent relationship with the new MSP, Org short name would like to understand the cost model for the services provided by the prospective MSP, so that changes to the environment can be seen to have a predictable effect on pricing and will not require a renegotiation of the Managed Services Agreement.

When changes occur, services and cost should easily adjust in line with previously defined and agreed parameters. This will provide certainty for both the MSP and Org short name and allow the internal ICT team to present a robust and scalable cost model to the business when changes are planned.

Org short name would like the prospective Service Provider to present their cost model. This model must reflect the support cost for casual and part time staff (vs. FTE), and for corporate and VIP staff vs. frontline staff, plus all devices, both physical and virtual.

Org short name would also look favourably at the suggestion of “Open Book Pricing” for hardware and software purchases, where one or more pre-defined and agreed mark-up percentages on the MSP’s procurement cost could streamline the repeat purchasing of ICT components and services by reducing the need for multiple quotes.

## MSP Response format and required information

Potential MSP’s are to supply a proposal that closely follows the outline below. Proposals that do not follow the outline will be harder to evaluate by the selection committee and may result in the MSP being excluded from consideration without notice.

We have produced the table below which you can use to manage the construction of your response.

| Section or Component Description | Done? |
| --- | --- |
|  |  |
| Executive Summary |  |
| Indicate your understanding of the challenge and the headline points of your response in two pages max. Do not include price. |  |
|  |  |
| Background to your business |  |
| Please describe the history of the company, its owners and its business focus over the last 5 years. |  |
| Include a legible chart of your organisational structure with respect to your business related to ICT managed services solutions. List the numbers of staff delivering ICT managed services. |  |
| Describe how your business will benefit from the proposed relationship with Org short name, and vice versa. |  |
| Describe the key risks of the proposed relationship to Org short name that you can foresee, and how they can and will be mitigated. |  |
| Describe the current key relationships of your organisation with suppliers and partners, including and industry-recognised certifications held. |  |
| Please describe relationships with third party suppliers used to deliver services covered by this proposal, including access to local service providers for any on-site required support in all Org short name’s service locations. Be sure to name any sub-contractors and provide CV’s of their key technical staff members. |  |
| Please provide an indication of your financial stability by providing a letter from a certified or chartered accountant or your Chief Financial Officer attesting to your current and anticipated financial health and indicating both your prior financial year turnover and net profit. |  |
|  |  |
| Technology Experience |  |
| This is where you have to name the technologies that are of key importance to the success of your new managed services relationship and ask the potential MSP’s to tell you about their experience. If you have conducted an Initial Planning Study, you will be able to nominate them with confidence where indicated below. |  |
| Please describe your experience in the following technologies: |  |
| Add technology description here. |  |
| Add technology description here. |  |
| Add technology description here. |  |
|  |  |
| Business Experience: |  |
| Decide how strict you want to be in working with an MSP that has direct experience in your industry and modify the sentence below to suit your decision. |  |
| Please describe your business experience in working with customers in the name your industry sector or similar industry by supplying the following details of prior customers in your proposal. |  |
| Customer name and headquartersStart and duration of service agreementServices provided (location(s), scope and technology)Size of the service e.g. Number of users, devices and servers supported, etc.Issues faced and the solutions implemented to successfully resolve those issues |  |
| Description of the proposed service team |  |
| Please provide CV’s no longer than one page each for the key team members who will work on our onboarding and ongoing managed services. Include links to staff LinkedIn profiles.Service Delivery ManagerProject ManagerProject Team leadService Desk ManagerLead EngineerAccount ManagerAny otherBe sure to describe the team members’ experience with the key technologies listed above. |  |
| Description of the Service Delivery Tools, Methodology and Processes |  |
| Please describe the included and excluded services that fall within and outside of your Managed Service offering. |  |
| Outline the methods that can be used to contact you and your team. |  |
| Describe the escalation process for VIP’s and urgent matters. |  |
| Describe the Account Management processes Org short name can expect. |  |
| Please describe the vendors of any software you intend to implement to facilitate service delivery, cybersecurity, asset management etc. |  |
| Which ITSM system is utilised by your organisation? To what degree will the ITSM be accessible by Org short name during the contracted support period? |  |
| Please describe your proposed SLA’s for Acknowledgement, Assignment and Remediation activity of support requests. Note that you may wish to specify your preferred SLA’s and ask the respondents to confirm they can deliver against them – that is fine and will ensure you can compare apples with apples. Remember though, the tighter the timeframes you specify, the higher the price you should expect to pay, because the more resources will need to be directed at your IT environment.Also note that we have not suggested that you should ask for a Resolution SLA that would establish a timeframe within which all service requests are to be finalised. Promising a resolution timeframe is quite hard for MSP’s to comply with, as some items are completely outside the MSP’s control, such as the network of a data carrier, or a malware attack that has to be investigated in forensic detail. You can ask for a commitment to a given timeframe, but don’t be surprised if the MSP’s who respond add a caveat that only XX% of tickets can meet that resolution timeframe. |  |
| Please describe your response to the Information Security requirements specified in the RFP. You can [find them here](#_Information_Security). |  |
| Please describe how your organisation performs network, endpoint and application Monitoring, Alerting and Response to alerts generated by monitoring agents. |  |
| Please describe your proposed backup and restoration process, including the RPO and RTO you can deliver within the proposed service? |  |
| Please describe your proposed services with respect to the creation and implementation of a Disaster recovery and Business Continuity plan for Org short name |  |
| Please describe your Patching and Update process and which are covered by your proposed Managed Service? (Patching, minor updates, major updates). |  |
| Please describe your hours of service including weekend, public holiday and after hours response. |  |
| Please disclose your current first contact ticket resolution rate and illustrate your process to promote and keep first contact resolutions high. |  |
| Please describe your Change Management Process. |  |
| Please describe how you will deliver a seamless handover for the management of Org short name's existing contracts - e.g. voice and network services. |  |
| Please describe your Quality Management accreditation status. |  |
| Please describe your Information Security accreditation status. |  |
| Please describe your continuous improvement process. |  |
| Onboarding |  |
| Please describe the proposed onboarding and support transition process, with emphasis on how you will make it a seamless process for Org short name. Be sure to describe the information and staff resources you would require from Org short name. |  |
| Please describe the Project Management methodologies you propose to use. |  |
| Compliance |  |
| Please confirm public and professional liability cover with the following limits1. Professional Indemnity. At least $10m any one claim and at least $20m overall cover
2. Public Liability. $20m any one claim.
3. WorkCover insurance (or state equivalent)
4. Please include a certificate of currency for all insurance products with your proposal.
 |  |
| Please explicitly confirm all staff and sub-contract staff members will participate in undertaking a police check. |  |
| (Add any other references to checks as necessary eg. Working with Children, Construction Safety, Mine Safety) |  |
| Customer Satisfaction |  |
| Please reveal your Net Promoter Score (or aligned customer satisfaction metric) combined across all clients for the past six months. |  |
| Disclosures |  |
| Please describe any significant events in the past 36 months that may affect your organisation’s financial viability, operations and service delivery. |  |
| Please make a statement about the financial viability of your operation and include a letter from your CFO, Director of Finance or public practising accountant attesting to your financial viability. |  |
| Please state whether the organisation is currently the target or lead in any merger/acquisition activity. |  |
| Investment |  |
| Describe the onboarding project’s costs. |  |
| Describe the required investment for the ongoing managed service, how it is calculated and how it will scale up or down depending on Org short name’s needs and staffing changes. Please present monthly recurring costs as both a total and a per-user, per-month figure. |  |
| If significant differences exist between the current and proposed future state of Org short name’s IT environment, please provide a different pricing model covering each state. |  |
| Also describe what periodic adjustments such as CPI are considered and when they might apply. Specify fixed versus variable costs and recurring versus one-off charges. Quote all prices as ex-GST. |  |
| Where remediation projects can be specified, provide an estimate of the project costs and project duration for each separately. |  |
| Please specify your hourly rates for ad hoc work not covered by the Managed Service Agreement or Onboarding project estimate. |  |
| References |  |
| Asking for references up front helps you qualify out MSP’s who don’t have a successful history of service provision. |  |
| Please provide three reference customers that can be contacted if, and when, your proposal is shortlisted. They will only be contacted at that point, and you will be notified in advance. Note that submissions along the lines of “referees to be provided on request” will invalidate your proposal. |  |
| Organisation name:Name and position of contact person:Phone and email:Services Provided:Dates when services commenced and ceased: |  |
| Master Service Agreement |  |
| Please provide a copy of your master service agreement. Exchanging this document now means fewer hold-ups later in the process. |  |
| Alignment with Org short name |  |
| Please demonstrate your ability to align with the values and vision of Org short name |  |
| Please indicate your agreement to adhere to Org short name’s Code of Conduct / Organisational Policies. (Note that you will need to publish your Code of Conduct and/or Organisational Policies with your Request for Proposal to help MSP’s conform to this item). |  |
| Please indicate your agreement to participate in Org short name’s contractor induction process. |  |
| Miscellaneous |  |
| Please provide any other information you feel should be considered in our evaluation. |  |

## Proposal Evaluation Process

During the selection process [Organisation full name] will evaluate the following information:

1. Review of the information and documents provided by the MSP as part of the proposal.
2. Gathering and analysis of information provided by the MSP’s referees.
3. Additional information provided by shortlisted MSP’s before, during or after the presentation given to [Organisation full name].

## Evaluation Criteria

[Organisation full name] will use the following as its basis for selection criteria. The final selection of the successful MSP is at the full discretion of [Organisation full name]. [Organisation full name] reserves the right to not select any of the applicant MSP’s or elect to negotiate discrete services from more than one of the potential providers where appropriate.

1. Value for money.
2. Alignment of culture and values between the organisations.
3. Track record and experience in working with [name your industry sector, e.g. Not for Profits] in both standalone projects and managed service provision.
4. Demonstrated commitment to delivering quality customer service.
5. Demonstrated commitment to Information Security
6. Demonstrated compliance with relevant legislation and security standards.
7. Innovation and alignment to industry best practice IT Service Management frameworks.
8. Evaluation of the financial stability and ongoing capability of the MSP.
9. Overall investment and contract terms put forward by the MSP.
10. Timing of the suggested onboarding and remediation activity and when agreed managed service levels can take effect.

## Thank-you

[Organisation full name] recognises and thanks you for the investment of time and effort to respond to our Request for Proposal. We understand the care and expertise that goes into crafting your response and would like to thank-you for undertaking to deliver a proposal.

## Appendix 1. Staff, Devices, Networks and Servers - Overview

(current state)

If you would prefer to place all this detail at the end of the document, you can elect to do so here. Otherwise, delete this section and add detail [earlier in the document](#_Current_ICT_Setup).

This is where you can give all the details that you would like the potential MSP’s to know about your ICT environment. The more they know, the more accurate their quoted fees will be.

If you are unsure how best to describe the environment, perhaps consider splitting your RFQ into two stages – an Initial Planning Study and the Managed and Project Services decision. The IPS will provide all the detail you need to run an effective RFQ process for the Managed and Project Services decision. Call us to discuss on 1300 667 871.

Here are some starter labels. Be sure to mention quantity, software, license statuses, age of devices and locations if that’s relevant.

|  |  |
| --- | --- |
| Platform Element | Details |
| Staff | Total Staff Approx: XXXApprox XX Full Time staff, XX Part Time staff, XX Casual.Indicate what percentage of each type of staff member needs access to a dedicated versus shared PC. Eg. If you have 100 staff, but 20 are part-time, you may only need 90 PC’s as 20 are shared (80 + 10 Full-time equivalent) |
| Server | Describe the following:How many serversWhat brand and what are the specs for each – Operating system, memory, CPU? Consolidate the information where possible – eg. If all servers are the same spec, you can just tell the reader how many you have rather than repeating the same specs XX times.Where are the servers located?Which are physical versus virtual?What is the current backup regime? |
| Data Centre locations | Where are your data centres? What brand (if public cloud) and where do you connect with them? |
| User devices | This is where you will describe the user endpoints that access your networkTypes: Desktops / Laptops / Tablets / PhonesBrandsModelsNumbersAre they company-owned or BYOD?For mobile devices (notebooks and phones) how do you control their access to organisational resources? Do you use Microsoft Endpoint Manager (Intune) or similar?How do your users access their productivity applications like Word and Excel or Adobe Creative Suite etc? Are they locally installed or accessed via cloud services?Indicate how many endpoints are active. If you plan to grow, provide an estimate of growth in Year 1. |
| WAN | Describe your network. Describe the use and specs of fibre, wireless or other connection that each site uses.Who supplies your Internet services? If you have more than one contract, when do they each expire? Do you have private, dedicated links or do you go via public Internet?Are remote sites able to access Internet directly or do they get it through Head Office? |
| LAN | Describe your Local Area Networks per site. What class of network addressing do you use? What devices are connected to your LANs?What wireless access points do you use for Wi-Fi? Brand and model number will help.What security standards around connection are present in the wi-fi network? Eg. Do you have a guest network that is restricted in the services it can connect to, or can anyone who joins the network see all devices?How are edge switches and access points managed? |
| Switches/Firewalls | Describe all the switches and firewalls in use, both on-premises and cloud-based. Indicate which is which and where they are located. |
| Wi-Fi | How many access points? What brand? |
| Phones | What kind of phone system does the organisation run? What brand and model are your handsets, if you still use those? |
| Active Directory | How many domain controllers do you have? Where is it / are they located and what do they each host?How many active staff accounts are there? Note that this may be different to the number of current users on staff.How many inactive accounts? |
| Email | How do you run your email? An Exchange server? Google Mail? Something else? Where is your exchange located?What, if any, protection do you have running on your mail services? |
| Printers | How many printers do you have, what brands and models are they and where are they located?Indicate if they are owned or leased. If they are leased, are you paying for the lease through toner consumption? Do you also receive maintenance services under your current agreement?Indicate if you would like printing supply management (toners and repairs) to be part of the managed services you are seeking.If you are already under a managed service agreement for your printers, but you would like to switch, indicate when the current contract is set to expire. |
| Specialist Hardware | Such as a CCTV system or factory technology you would like your MSP to play a role in managing. |

## Appendix 2. Applications and Services

As with the previous Appendix, you can either choose to add your ICT environment details at the end of the document, or [earlier in the piece](#_Current_ICT_Setup). Delete whichever does not apply.

Following on from the hardware environment description, this is your opportunity to ensure the potential MSP’s understand your applications and other services.

As above, if you’re not quite sure how best to describe your applications and services, get in touch with Computer One and we will help you with the specification by conducting the Initial Planning Study and setting up your Managed and Project Services RFQ for success.

Here are some starter items.

|  |  |
| --- | --- |
| Application | Details |
| Microsoft Office 365 | Indicate how many 365-based products you have licensed and what version of 365 software they areEg. Microsoft 365 Business Premium, Business Basic, Enterprise E3, E5 etc. |
| ERP Software  | Do you use a particular piece of software to run your business, like an ERP programme? This is where you would describe it. |
| Security | Indicate the security products you use. This may be anti-malware, endpoint detection and response, mail protection, security incident and event management etc. |
| Accounting package |  |
| Anti-malware |  |
| Backup Software |  |
| Email | Which email platform do you use? |
| File Server  |  |
| IT Service Management |  |
| Network agents |  |
| Payroll software |  |
| Software Asset Management system |  |
| Telephony | For those companies using a softphone application |
| Terminal Services |  |
| Miscellaneous on-premise applications | Specialist video editing software is an example of what you would put here. Local security software that runs a video surveillance system is another. |
| Miscellaneous Software-as-a-Service applications | Applications like Zoom video conferencing etc. Cloud-based security software |