

Evaluating
an IT Supplier

Micro to Small

Contents

[This tool in a nutshell 2](#_Toc162006985)

[Why does it matter? 2](#_Toc162006986)

[How to use this tool 2](#_Toc162006987)

[Where to find this checklist 3](#_Toc162006988)

[Section 1: Questions to ask your IT supplier about their own good information security practices. 4](#_Toc162006989)

[Section 2: Questions to ask your IT Supplier about how they will support your organisation to keep the information you hold and your systems secure and available. 7](#_Toc162006990)

[Appendix 1: Questions mapped to HISF 16](#_Toc162006991)

# This tool in a nutshell

This tool contains questions and sample answers to use when engaging or evaluating an Information Technology (IT) supplier. The tool helps you understand how well the supplier is supporting you to achieve a high information security maturity level, defined by the HISO 10029.2:2023 Health Information Security Framework Guidance for Micro to Small Organisations.

# Why does it matter?

Smaller organisations rely heavily on their IT supplier to setup, maintain and support their digital footprint. Asking the right questions when selecting an IT supplier can make a big difference in securing your information and systems.

There are two aspects to consider when you are getting IT services from a supplier:

1. What are the secure practices that the IT supplier has in their own operations? For example, are they screening and training their own staff, and do they have backups and incident response plans in place should their own organisation suffer a cyber-attack or outage?
2. How are services provided to you securely by the IT supplier? For example, how do they provide and support all your hardware and software, monitor your network, and patch your systems to keep them up to date and secure?

By confirming that a potential IT supplier is managing both aspects of security well, you can reduce the risk of events that could result in system outages, unauthorised access to medical information, impacts to patient safety or a financial loss to your organisation.

# How to use this tool

We suggest you conduct an interview with your potential IT supplier and review each question. Each question has a table showing you what a good response looks like. Ultimately the decision of whether to use an IT supplier or work with them to uplift your security maturity lies with you.

For any question they answer “Not Yet” or “No” to, you should consider what that could mean for your organisation. The template provides general guidance in relation to IT security and is not intended to be an exhaustive list of security considerations.

# Where to find this checklist

This checklist and more like it are published on the Te Whatu Ora Cyber Hub.

# Section 1: Questions to ask your IT supplier about their own good information security practices.

|  |
| --- |
| 1. Does your organisation comply with HISF guidance for suppliers? Or an equivalent standard like ISO27001 or SOC 2 Type 2?
 |

What good looks like

|  |  |
| --- | --- |
| Standard | * They provide you with an independent report showing their compliance with the HISF Guidelines for suppliers or another equivalent standard.

If they can provide this report, skip section 1 and go straight to section 2.* Understanding or knowledge of these standards is shown.
* Their website and documentation references these standards.
 |

|  |
| --- |
| 1. How large is your company in terms of staff? And how long have you been providing IT services?
 |

What to look for

|  |  |
| --- | --- |
| Number of Staff | * Having around-the-clock support will require more staff.
* An organisation with more staff can become specialised with information security expertise.
 |
| Years in Business | * Longer time in business allows for more mature information security practices to be in place.
 |

|  |
| --- |
| 1. How do you screen your staff before you hire them?
 |

What good looks like

|  |  |
| --- | --- |
| Screening | * All staff at your IT supplier should be screened in an appropriate manner such as Ministry of Justice criminal record check, reference checks, etc.
 |

|  |
| --- |
| 1. What training and awareness do you provide your staff relating to information security?
 |

What good looks like

|  |  |
| --- | --- |
| Training | * All staff should be continuously trained in good information security practices, as relevant to their roles. Such as good email security practices such as not clicking on links with unusual domains.
 |

|  |
| --- |
| 1. What are the key components of your information security policy? Who is given responsibility for information security in your organisation?
 |

What good looks like

|  |  |
| --- | --- |
| Information Security Policy | * Look for topics such as security principles, standards, governance, responsibility, accountability, monitoring, review and update.
* Look at the Information Security Policy guidance and template provided for Micro to Small Businesses by Te Whatu Ora for more examples.
 |
| Security Responsibility | * Having a role where ‘Security’ is specified in the job title shows a commitment to a strong security culture.
* For smaller organisations some roles may also include security as their responsibility. The thing to look out for is whether security is everyone’s responsibility, and no specific accountability is shown.
 |

|  |
| --- |
| 1. What due diligence do you complete for your third-party suppliers? And do you include any information security clauses in your contractual agreements?
 |

What good looks like

|  |  |
| --- | --- |
| Due Diligence Process | * A documented process that includes requesting evidence such as a penetration test report.
* Due diligence process includes a Security Risk Assessment (SRA).
 |

# Section 2: Questions to ask your IT Supplier about how they will support your organisation to keep the information you hold and your systems secure and available.

|  |
| --- |
| 1. How do you track the inventory of hardware and software that you provide and manage for us?
 |

What good looks like

|  |  |
| --- | --- |
| Asset Register | * A detailed software and hardware asset register helps ensure assets are not forgotten about, and are kept up to date and secured.
* The supplier should have a separate, detailed asset register for their own internal assets and for those provided to each of their clients.
 |

|  |
| --- |
| 1. For Question 8, answer the questions for any hardware which will be provided or maintained by the IT supplier.

For example, servers, routers, printers, Wireless Access Points, laptops, phones, fax machines. |

|  |
| --- |
| * 1. How do you ensure our hardware stays up to date, including hardware refreshing where appropriate?
 |

What good looks like

|  |  |
| --- | --- |
| Hardware Updates | * The IT supplier regularly updates all hardware assets.
* Where possible, automatic updates are enabled.
* You are notified of potential downtime of hardware for updates.
 |
| Patching | * A patch is a small update that is designed to fix bugs or security vulnerabilities quickly.
* The IT supplier has a plan for patching that includes different timeframes depending on how important the patch is.
* Critical patches should be applied as soon as possible, preferably within a day or two.
 |
| Hardware Refreshing | * When hardware can no longer be updated or is no longer supported, it needs to be replaced.
* Hardware assets are replaced on a set schedule, before their support expires.
 |

|  |
| --- |
| * 1. How do we request new software is installed on hardware managed by the IT Supplier?
 |

What good looks like

|  |  |
| --- | --- |
| Safe software installs | * Ensure that employees can't accidentally install malware or inappropriate software.
* A formal process is in place for staff to request new software, that includes information security due diligence.
* Only IT Staff can install software.
 |

|  |
| --- |
| * 1. What anti-malware software is installed on hardware devices and how is it kept current? And what happens if one gets infected with malware?
 |

What good looks like

|  |  |
| --- | --- |
| Anti-malware | * Anti-malware software is installed.
* The software is monitored remotely by your IT supplier.
* A documented process is in place to handle infected devices to ensure the malware does not propagate.
 |

|  |
| --- |
| * 1. If a device were to be lost or stolen, what process should we follow?
 |

What good looks like

|  |  |
| --- | --- |
| Process for lost devices | * An easy-to-follow process is in place.
* Lost devices are remotely erased to protect sensitive information.
 |

|  |
| --- |
| * 1. How do you securely configure the hardware?
 |

What good looks like

|  |  |
| --- | --- |
| Configuration | * Understanding or knowledge of these requirements are shown.
* All devices managed by the IT supplier is configured according to international standards like CIS (Centre for Internet Security).
* The IT supplier can provide examples of how they implement these requirements.
 |

|  |
| --- |
| * 1. Is there either a VPN (Virtual Private Network) or a VDI (Virtual Desktop Interface) in use on computers to protect information in transit when working from home?
 |

About this question

You only need to ask this question if you or your staff work remotely. VPNs or VDIs are used to protect information in transit when the security of the network isn’t guaranteed.

What good looks like

|  |  |
| --- | --- |
| Remote Work Security Measures | * Importance of protecting information in transit is understood.
* A VPN or VDI is in use.
* For more information on how to allow staff to securely work from home, please see HISF Control HMS13.
 |

|  |
| --- |
| * 1. How are network services that transmit and receive health information kept secure?
 |

What good looks like

|  |  |
| --- | --- |
| Network Security Measures | * Guest Wi-Fi is separated from internal network Wi-Fi.
* Due diligence has been completed on the network.
 |

|  |
| --- |
| 1. How do you make sure the software that you supply or recommend keeps our information secure? Please use email options as one of your examples.
 |

What good looks like

|  |  |
| --- | --- |
| Supply process for software | * The process considers the information security viability of a desired software, considering key aspects such as whether the product provides MFA, backup and restore functionality.
* The IT supplier recommends you always use a licensed, paid-for version of the software as it includes stronger contractual obligations and commitment to help with security requirements.
 |

|  |
| --- |
| 1. If your supplier is developing any custom software or applications for you, ask the following question
 |

|  |
| --- |
| * 1. How do you make sure that software you develop for us keeps our information secure? And is developed securely?
 |

What good looks like

|  |  |
| --- | --- |
| Design Phase | * Information security is considered early in the design phase.
* Coding guidelines are in use and informed by standards such as the OWASP Developer guide.
* Technologies are analysed for potential business, customer and security risks before use.
 |
| Development Phase | * Security testing is conducted on the software to identify vulnerabilities.
* Code reviews are conducted.
 |
| Support Phase | * Software supports the organisation’s audit log requirements.
* Software supports secure authentication (Single-Sign-On, MFA)
 |

|  |
| --- |
| 1. If your IT supplier is also providing your website, ask the following question
 |

|  |
| --- |
| * 1. What security measures are in place for the website?
 |

What good looks like

|  |  |
| --- | --- |
| Denial of Service (DoS) Protection | * A WAF (Web Application Firewall) is in front of the website.
* The website is being delivered using a CDN (Content Delivery Network).
 |
| Encryption  | The Website is using HTTPS with a NZISM- or HISF- compliant encryption.  |

|  |
| --- |
| 1. How often are backups conducted and verified, and where are they stored?
 |

What good looks like

|  |  |
| --- | --- |
| Frequency | * Backups are done automatically, with a frequency that reflects the importance of the information. For example, would you be able to function and recover if you lost an hour’s worth of data, or should you backup your data more frequently?
 |
| Backup Validation | * Backups, particularly of health information, should be complete, secure, and able to be restored without undue delay.
* The IT supplier tests that the backups can be used to restore information.
* Backups are encrypted.
* This testing is conducted at least twice a year.
 |
| Backup Location | * Backups are not stored on site.
* Backups are stored in either New Zealand or Australia.
 |

|  |
| --- |
| 1. Is data encrypted (in both transit and in storage) and what algorithms are used?
 |

What good looks like

|  |  |
| --- | --- |
| Encryption | * All data in transit or at rest is encrypted using NZISM- or HISF-compliant algorithms.
* Be wary of IT suppliers that use TLS 1.1 or AES 128, which are outdated encryption algorithms.
 |

|  |
| --- |
| 1. Do you follow the principle of least privilege? Can you explain who has access to my information? Your staff, your 3rd party suppliers?
 |

What good looks like

|  |  |
| --- | --- |
| Principle of least privilege | * Users of the system are given just enough access for them to perform their role, and no more.
 |
| System Access Control | * Clear processes exist for giving IT suppliers access to sensitive information.
* All activities are logged and audited.
* There is a reporting system that allows regular and ad hoc reporting to be conducted, to view and correlate IT supplier activities.
 |

|  |
| --- |
| 1. How does your product or service support strong and complex passwords, and the use of Multifactor Authentication (MFA)?
 |

What good looks like

|  |  |
| --- | --- |
| Passwords | * The use of a complex passphrase is supported.
* The minimum length and combination of characters in passphrases is enforced.
* Users are prevented from reusing recent passwords.
* Users are automatically logged out after a certain period.
 |
| Multi-Factor Authentication | * Multifactor Authentication (MFA) is enforced.
 |

|  |
| --- |
| 1. How do you monitor the product or service for unusual activity, and when and how do you contact us if you detect something unusual?
 |

What good looks like

|  |  |
| --- | --- |
| Monitoring  | * Time stamped logs are available on request for failed and successful logons, user activity, changes to privileges, system changes, and network activity.
* Regular reporting on logged activity is available.
 |
| Reporting Process  | * The IT supplier has clear service level expectations for contacting you if they identify unusual activity and has a proactive and customer-centred approach.
 |

|  |
| --- |
| 1. What support do you provide should we need to conduct an investigation or report a data breach?
 |

What good looks like

|  |  |
| --- | --- |
| Support Provided | * A documented data breach support process is provided, with clear service level expectations.
* A support team can be made available to assist with investigations, if required.
 |

|  |
| --- |
| 1. Has your organisation ever handled an information security incident for an organisation before? And if not, how are you prepared should one occur?
 |

What good looks like

|  |  |
| --- | --- |
| Information Security Incident | * Companies that have prepared incident response plans - with defined roles and responsibilities, steps to contain a breach, and appropriate notification processes in place - are more likely to be able to recover quickly and reduce the impact of a breach.
* If the IT supplier has never handled an incident, tabletop exercises are a great way to prepare for an incident, should one occur.
 |

# Appendix 1: Questions mapped to HISF

## Section 1: Questions to ask your IT supplier about their own good information security practices.

| Question  | HISF Requirement it maps to |
| --- | --- |
| 1. Does your organisation comply with HISF guidance for suppliers? Or an equivalent standard like ISO27001 or SOC Type 2?
 | HMS01, HMS02 |
| 1. How large is your company in terms of headcount? And how long have you been providing IT services?
 | N/A |
| 1. What training and awareness do you provide your staff relating to information security?
 | HMS01 |
| 1. How do you screen your staff before you hire them?
 | HMS01 |
| 1. What are the key components of your information security policy? Who is given responsibility for information security in your organisation?
 | HMS02 |
| 1. What due diligence do you complete for your third-party suppliers? And do you include any information security clauses in your contractual agreements?
 | HMS04, HMS05, HMS06, HMS15 |

## Section 2: Questions to ask to determine how the IT Supplier will support your organisation to keep the information you hold and your systems secure.

| Question  | HISF Requirement it maps to |
| --- | --- |
| 1. How do you track the inventory of hardware and software that you provide and manage for us?
 | HMS03 |
| 1. What hardware, if any, do you provide or maintain for us? Such as laptops, servers, printers, routers.
 | N/A |
| * 1. How do you ensure our hardware stays up to date, including hardware refreshing where appropriate?
 | HMS08  |
| 7.2 What is our process for getting new software installed on hardware that you manage? | HMS09  |
| 7.3 Do you have anti-malware software on the hardware devices? And what happens if one gets infected with malware? | HMS10  |
| 7.4 If a device were to be lost or get stolen, what process should we follow? | HMS12  |
| 7.5 How do you securely configure the hardware? | HMS12, HMS09 |
| 7.6 Is there either a VPN (Virtual Private Network) or a VDI (Virtual Desktop Interface) in use on computers to protect information in transit when working from home? | HMS13  |
| 7.7 How are network services that transmit and receive health information kept secure? | HMS15, HMS16 |
| 1. How do you make sure the software that you supply or recommend keeps our information secure?
 | HMS14 |
| 1. If your supplier is developing any custom software or applications for you, ask the following question.
 | N/A |
| * 1. How do you make sure that software you develop for us keeps our information secure? And is developed securely?
 | Not in guidance for micro to small. Can be found in Supplier guidance HSUP14. |
| 10 If your IT supplier is also providing your website, ask the following question. | N/A |
| 10.1 What security measures are in place for the website? | HMS17  |
| 1. How often are backups conducted and verified, and where are they stored?
 | HMS11 |
| 1. Is data encrypted (in both transit and in storage) and what algorithms are used?
 | HMS06, HMS12 |
| 1. Do you follow the principle of least privilege? Can you explain who has access to my information? Your staff, your 3rd party suppliers?
 | HMS07 |
| 1. How does your product or service support strong and complex passwords, and the use of Multifactor Authentication (MFA)?
 | HMS07, HMS14 |
| 1. How do you monitor the product or service for unusual activity, and when and how do you contact us if you detect something unusual?
 | HMS19 |
| 1. What support do you provide should we need to conduct an investigation or report a data breach?
 | HMS01, HMS18, HMS20 |
| 1. Has your organisation ever handled an information security incident for an organisation before? And if not, how are you prepared, should one occur?
 | HMS20 |