Simply Energy

NZ Government CIO
Cloud Security Questionnaire Response

Site iQ

Document Overview

This document contains responses to the New Zealand Government's Chief Information Officer's questionnaire on risk discovery for public cloud services. Specifically, it addresses questions related to Site iQ, a cloud-based solution for plug-load and building energy management. The responses are aligned with the guidelines provided at the following link from digital.govt.nz.

How to read this document

This document outlines Simply Energy's responses to the service provider questions from the unsorted format referenced on the digital.govt.nz website, specifically regarding risk discovery for public cloud services. Each question in the document includes:

- the full question,
- a detailed description and context of the question,
- the type of risk addressed,
- the control category; and,
- Simply Energy's response.

While this document is intended to address a questionnaire for the public sector, it can also be shared with private sector organisations considering Site iQ, to provide insights into the product's cloud risk and security management.

Please note that responses are not provided for questions 1–15, 36, 55, and 80, as these are the agencies' responsibility to answer.

Background

Site iQ provides a simple solution for understanding occupancy and reducing energy, equipment, and space costs in buildings. Its controls and insights help businesses optimise the use of their equipment and workspaces.

Installed on-site, smart plugs collect data on energy consumption from connected equipment, including when and how much energy they use. This data is sent to an online analytics platform, which offers valuable insights into equipment usage, space utilisation, and workstation occupancy. The platform also provides tools to set controls for more efficient equipment operation.

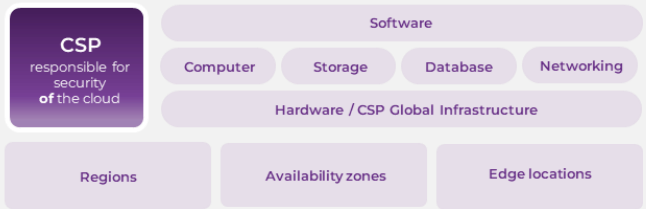
Automated controls can reduce equipment energy consumption by up to 40%*.

*Based on existing customer installations.

Site iQ third-party providers

Sapient is Simply Energy's primary third-party provider, responsible for delivering the essential applications and cloud infrastructure used by Site iQ. Sapient uses TP-Link hardware to collect energy usage data from plug loads and stores this information within its own cloud infrastructure. Specifically, Sapient uses the TP-Link Kasa and Tapo platforms to transmit plug energy usage data through its cloud services.

Both Sapient and Simply Energy services rely on cloud service providers (CSPs) to ensure secure delivery of the solution to customers.



Questionnaire responses

16. Is the registered head office of the service provider clear?

Risk type	Control Category
Control of information	Governance

Context:

Select service providers registered in appropriate jurisdictions.

The jurisdiction in which the service provider's head office is registered may affect how the provider treats customer data.

Response:

Simply Energy's head office is located in Wellington, New Zealand.

Level 1, 92 Abel Smith Street
Te Aro
Wellington 6011

17. Is it clear which countries are the cloud services delivered from?

Risk type	Control Category
Control of information	Architectural

Context:

Identify the countries that the cloud service is delivered from.

Cloud services are typically delivered from countries other than the location of the provider's head office. This might affect how the information is managed or the agency's control of it.

Response:

Simply Energy uses a third-party provider, Sapient, to deliver the Site iQ control and reporting platform. Sapient is located in Philadelphia, USA, and its primary data centre facilities are also located within the United States. Sapient uses TP-Link – Kasa Smart hardware and cloud infrastructure to record and control energy consumption at a plug load level. TP-Link Research America Corporation is located at 245 Charcot Avenue, San Jose, CA 95131, USA and Kasa smart data is stored in data facilities in the United States. Other Simply Energy digital services will be provided to customers from the Google data centre facilities located in Sydney, Australia.

18. Is it clear in which legal jurisdictions the agency's data will be stored and processed?

Risk type	Control Category

Control of information	Governance

Context:

Identify the countries where the cloud services are delivered.

Cloud services are typically delivered from countries other than the location of the provider's head office. This might affect how the information is managed or the agency's control of it.

Response:

Yes, as per question 17, the agency's primary data location will be within the United States or Australia.

19. Does the service provider allow its customers to specify the locations where their data can and cannot be stored and processed?

Risk type	**Control Category**
Control of information	Architectural

Context:

Assess the suitability of jurisdictions used to store and process information.

Information may be subject to the laws of the locations in which it's stored and processed.

Response:

No, only the locations specified per provider are available.

Simply Energy – Sydney, Australia.

Sapient – USA.

20. Have the laws of the country or countries where the data will be stored and processed been reviewed to assess how they could affect the security and privacy of the information?

Risk type	**Control Category**
Control of information	Governance

Context:

The jurisdictions where the data will be stored or processed may have laws that affect agency data, for example, by:

- *requiring the provider to disclose customer information if requested by the government or law enforcement; and,*

– *having privacy laws in that jurisdiction that may not meet the standard required by the Privacy Act 2020.*

Response:

Sapient and TP-Link's privacy policies and terms of use advise customers to consult their own legal advisors to fully understand the data storage and processing laws applicable in their country.

Sapient's policy on international users can be found below:

"The Service is controlled, operated, and administered by Sapient from our offices within the USA. If you access the Service from a location outside the USA, you are responsible for compliance with all local laws. You agree that you will not use the Sapient Content accessed through Sapient Industries in any country or in any manner prohibited by any applicable laws, restrictions or regulations."

21. Are customers able to negotiate with the service provider to ensure that sufficient privacy protections are specified in the contract to meet the requirements of the Privacy Act 2020?

Risk type	**Control Category**
Control of information	Contract

Context:

Ensure that contracts enforce sufficient privacy protections to meet the requirements of the Privacy Act 2020.

You are responsible for the privacy of personal information, even when it's being held or managed by service providers. You must ensure that your service provider will manage and protect personal information in a manner consistent with the Privacy Act 2020, even when the information or service provider is overseas. The Privacy Commissioner provides model contract clauses you can use.

Response:

In Simply Energy's view, the privacy laws in Australia provide similar protections to New Zealand's privacy laws in instances where they apply. The privacy laws between New Zealand and the United States do not provide similar protections. Simply Energy recommends that customers should seek their own legal advice to fully understand the laws of the country where the data will be stored and processed.

Additionally, given the context of the Site iQ product, the risk and level of personal data are relatively low as the overall capture of personal data is limited.

Simply Energy is willing to engage and negotiate with customers to help ensure their specific requirements on privacy are met.

22. Does the contract specify that the provider will only disclose information in response to a valid court order or another lawful access request?

Risk type	Control Category
Control of information	Contract

Context:

Ensure that contracts specify that the provider will only disclose information in response to a valid court order or another lawful access request.

Lawful access occurs when a third party, usually a law enforcement or national security agency, has a legal right to access the agency's data through the service provider in the performance of its responsibilities. This may or may not require a court order, and the provider may not be allowed to notify the agency if this occurs.

Response:

Yes, as per Clause 9a of the agreement:

a. *That information will not be disclosed by you or us except:*

   i. *as required by law;*

   ii. *as is necessary to satisfy the requirements of any regulatory agency or stock exchange;*

   iii. *where the other party otherwise agrees in writing;*

   iv. *is lawfully obtained from a third party who is not under any obligation of confidentiality or non-disclosure;*

   v. *as is necessary or provided for under the Agreement;*

   vi. *to your or our professional advisors and consultants; or*

   vii. *becomes publicly available through no fault or breach of the receiving party, including but not limited to information that enters the public domain without any wrongful act or omission by the receiving party.*

23. Does the provider inform their customers if they have to disclose information in response to a lawful access request?

Risk type	Control Category
Control of information	Contract

Context:

Where possible, the provider should notify the agency if its data is subject to a lawful access request.

Agencies may wish to know that their information has been subject to a lawful access request. In addition, agencies have obligations for information they have in their control. This may include obligations to notify others about the use and access of information. In some cases, the provider may be prevented from notifying the agency that a request has been made.

Response:

Yes, as per the previous response, see clause 9a of the Site iQ agreement.

24. Is the service provider's use of personal information clearly set out in its privacy policy?

Risk type	Control Category
Privacy	Contract

Context:

The provider must either agree through contract to make no use of personal information or clearly indicate what uses it intends so that the agency can decide if this meets agency obligations and needs.

Response:

Yes, please review our Privacy Policy and Terms of Use with specific reference to the Customer section:

Simply Energy Privacy Policy and Terms of Use

25. Does the service provider notify its customers if their data is accessed by, or disclosed to, an unauthorised party?

Risk type	Control Category
Incident recovery	Contract

Context:

The provider must either agree through contract to make no use of personal information or clearly indicate what uses it intends so that the agency can decide if this meets agency obligations and needs.

Response:

As per section 10 c of the Site iQ agreement:

If either Party becomes aware or suspects that any unauthorised person has obtained, attempted to obtain, or may obtain access to the Data or any other confidential information or has altered, used or attempted to use the Data or any other confidential information for purposes not authorised or permitted by the terms of this Agreement or that any Data or any

other confidential information has been lost, destroyed or otherwise made unavailable on a permanent or temporary basis without either parties prior written consent or if there is any near miss in relation to any of the foregoing ("**Security Breach**") in respect of this Agreement:

i. that party will, on becoming aware of such Security Breach, immediately notify the other party of that Security Breach;

ii. Both parties agree to:

1. take such steps as are available to it to identify any relevant unauthorised person(s);
2. contain and mitigate the Security Breach;
3. assess the nature of the Security Breach, including as to the type of information disclosed, lost, or accessed and the scope of any parties to which it may have been disclosed or accessed;
4. investigate the cause(s) of the Security Breach and, disclose details of all causes or likely causes of the Security Breach;
5. make all relevant personnel and Subcontractors available to assist with the consequences and implications arising from the Security Breach;
6. make such changes to its operations (at its own cost) that are necessary to prevent, as far as is practicable, the occurrence of the same or similar Security Breaches in the future; and

26. Does the service provider notify its customers if their data is accessed by, or disclosed to, an unauthorised party?

Risk type	**Control Category**
Incident recovery	Contract

Context:

The provider must either agree through contract to make no use of personal information or clearly indicate what uses it intends so that the agency can decide if this meets agency obligations and needs.

Response:

If customers believe that Simply Energy is not adhering to its privacy or security commitments, customers can contact us through one of the following methods:

Email:

Customers can email their concerns to solutions@simplyenergy.co.nz.

Webform:

Customers can submit a general enquiry using our online webform.

Post:

Customers can send their concerns to:

Site iQ

Level 1
92 Abel Smith Street
Te Aro
Wellington 6011

27. Does the service provider's terms of service and service level agreement (SLA) clearly define how the service protects the confidentiality, integrity and availability of all customer information entrusted to them — especially official information and the privacy of all personally identifiable information?

Risk type	Control Category
Governance	Contract

Context:

Contracts and SLAs should clearly define how the service protects the confidentiality, integrity, and availability of all customer information entrusted to it, especially official information and the privacy of all personally identifiable information.

Contracts and agreements should require service providers to meet the confidentiality (including privacy), integrity, and availability needs of all data.

Response:

Yes, confidentiality is referenced in clause 9a of the Site iQ agreement:

b. The Agreement and any information that has been provided under the Agreement by you or us that is not publicly available is confidential. That information will not be disclosed by you or us except:

- *i. as required by law;*
- *ii. as is necessary to satisfy the requirements of any regulatory agency or stock exchange;*
- *iii. where the other party otherwise agrees in writing;*
- *iv. is lawfully obtained from a third party who is not under any obligation of confidentiality or non-disclosure;*
- *v. as is necessary or provided for under the Agreement;*
- *vi. to your or our professional advisors and consultants; or*
- *vii. becomes publicly available through no fault or breach of the receiving party, including but not limited to information that enters the public domain without any wrongful act or omission by the receiving party.*

Availability is covered in Simply Energy Privacy Policy and Terms of Use under **Rights of access and correction.**

28. Does the service provider's terms of service specify that the agency will retain ownership of its data?

Risk type	Control Category
Governance	Contract

Context:

Contracts should include terms that specify that the agency will retain ownership of its data.

Agencies are obliged to maintain Crown ownership of data. The provider must comply with this obligation, or the agency must ensure that it can meet its obligation through another mechanism.

Response:

As per section 10b of the Site iQ agreement:

Both parties acknowledge that the data, in whatever form and on whatever media, remains the property of both parties or its licensors.

29. Will the service provider use the data for any purpose other than the delivery of the service?

Risk type	Control Category
Control of information	Contract

Context:

Contract terms should prevent the service provider from using data for any purpose other than the delivery of the service.

Agencies have obligations for data in their control. These may include limits on what the information can be used for and who it can be used by. These obligations may arise through different mechanisms, including legislation (for example, the Privacy Act), contracts, agreements made at the point of collection, or through reasonable expectations of behaviour by the Public Service.

Response:

Use of data is covered in Simply Energy's Privacy Policy and Terms of Use under our **Customers** section.

30. Is the service provider's service dependent on any third-party services?

Risk type	Control Category

Governance	Governance

Context:

Ensure that subcontractors and third-party services used by the provider meet the same expectations as the provider.

When a provider is dependent on another third party, the agency and its customers become dependent on that third party. It's necessary to understand that level of dependency and the risks it poses to the agency, its customers, and others.

Response:

Simply Energy is dependent on 2 third-party providers to deliver Site iQ.

Sapient Industries

Sapient is the service provider responsible for the Site IQ platform, including cloud storage, retention, and integration with TP-Link (Kasa).

TP-Link

TP-Link is the service provider responsible for the smart plug infrastructure and transmission of plug energy consumption to Sapient. This is achieved through the use of their Kasa Smart / Tapo platform. TP-Link and the Kasa / Tapo platform do not hold any customer-related information as this is retained within the Sapient platform.

Each party has dependencies on cloud service providers, Amazon (AWS), Azure or Google (GCP).

31. Does the service provider undergo regular assessment by an independent third party against an internationally recognised information security standard or framework?

Risk type	**Control Category**
Governance	Audit

Context:

An independent third party regularly assesses the provider and service against an internationally recognised information security standard or framework.

Independent reports and certifications give assurance that the provider meets a minimum security standard. The reports will describe the security controls and practices the provider has in place. Widely accepted standards include:

- *ISO 27001*
- *NIST Cybersecurity Framework (CSF)*
- *Cloud Security Alliance (CSA) STAR certification.*

An ISAE 3402 SOC 2 Type II report will describe how the provider's security controls have performed over time.

Response:

Sapient's systems are AICPA SOC 2, Type 1 Certified.

Sapient's systems and processes have undergone rigorous assessment by an independent third party, following the standards set by the American Institute of Certified Public Accountants (AICPA).

This assessment focuses on the design and implementation of its controls across AICPA's five Trust Services Criteria, ensuring they deliver the highest standards of security, availability, processing integrity, confidentiality, and privacy.

Sapient's SOC 2 Audit Report is available on request.

TP-Link is compliant with ISO 27001 and ISO27701, as indicated on its website:

"As a company compliant with ISO 27001 & ISO27701, TP-Link underscores its commitment to data confidentiality and integrity. We've earned trust and loyalty among stakeholders while adhering to all laws and regulations related to data protection. Recognizing the critical nature of data security, we strive to provide a reliable, always-connected lifestyle for our valued customers."

32. Can the agency review recent audit and certification reports, including the Statement of Applicability, before signing up for service?

Risk type	Control Category
Governance	Audit

Context:

Agencies can reasonably expect that when they choose to rely on independent third-party assurance activities, they will be provided with sufficient information to understand the full scope and findings of those activities.

If the provider does not make independent certification and compliance documents available for review, then you should consider requiring an independent audit.

Response:

Yes. We can provide a copy of Sapient's SOC 2 Audit Report on request.

33. Does the service provider's terms of service allow the agency to directly audit the implementation and management of the security measures that are in place to protect the service and the data held within it?

Risk type	Control Category

Governance	Audit

Context:

For higher-risk services or services where the agency has reason to have less confidence in the provider, the agency may need to directly audit the measures being used to secure the information it has in its control.

Response:

If required, Simply Energy can allow the agency to directly audit the implementation and management of security measures for Site iQ.

Simply Energy considers Site iQ to be a low-risk product because it handles only low-risk data and does not store any personal information about users (only email addresses and names for IAM).

34. Will the service provider enable potential customers to perform reference checks by providing the contact details of two or more of its current customers?

Risk type	**Control Category**
Governance	Audit

Context:

This will need to be handled on a case-by-case basis; for example, it'll depend on whether the current customer will allow direct contact.

Response:

Simply Energy allows prospective customers to engage with an existing customer as a reference check. If required, please discuss this with your point of contact at Simply Energy.

35. Is the service provider a signatory to the Cloud Computing Code of Practice?

Risk type	**Control Category**
Governance	Governance

Context:

The Cloud Computing Code of Practice provides a set of foundational expectations about what cloud providers will disclose to agencies and includes a complaints process. It allows agencies to have clarity about what information the provider will disclose to them. Agencies may still choose to request or perform independent assurance on any matters, including those which the providers have signed up to as part of the Code of Practice.

Response:

Yes, Simply Energy has multiple employees who have completed the Cloud Computing Code of Practice.

37. Does the cloud service support the agency's identity management strategy?

Risk type	Control Category
Unauthorised access	Governance

Context:

The service should support identity federation, authorisation and single sign-on that can integrate with the agency's directory and identity services.

Response:

No. At this time, Simply Energy and an agency administrator manage identity management and user access control. No single sign-on with integration capability is available.

38. Does the agency have an effective and audited internal process that ensures that identities are managed and protected throughout their lifecycle?

Risk type	Control Category
Unauthorised access	Governance

Context:

Have an effective and audited internal process that ensures that identities are managed and protected throughout their lifecycle.

Cloud services rely on the agency's identity records to enforce authorisation and access to services and information and maintain accurate records of user activity within the service. It's important that identity record maintenance is timely and accurate as users join, leave, or change roles within the service. Identity records must be protected to ensure their integrity.

Response:

Site iQ services support the maintenance of user permissions, roles, and active status during staff joins, changes, and exits. This is managed by system administrators only.

39. Are all passwords encrypted, especially system and service administrators, in accordance with the complexity requirements of the New Zealand Information Security Manual (NZISM)?

Risk type	Control Category
Unauthorised access	Access management

Context:

Passwords must be complex enough to resist discovery and must be appropriately hashed or encrypted when stored so they are not exposed in case of an incident. The NZISM sets minimum standards for encryption and complexity.

Response:

Yes, Site iQ services use encrypted password protection, which is in accordance with the NZISM's complexity requirements.

40. Does the service allow the use of multi-factor authentication?

Risk type	Control Category
Unauthorised access	Access management

Context:

The service should support identity federation, authorisation and single sign-on that can integrate with the agency's directory and identity services.

Response:

No. at this time, multi-factor authentication is not available within Site iQ services.

41. Does the independent audit and certification include an assessment of the security controls and practices related to the separation of tenant data?

Risk type	Control Category
Control of Information	Audit

Context:

Please check that the independent audit and certification include an assessment of the security controls and practices related to the separation of tenant data.

Agencies need to assure themselves that their data is not mixed with the data of other customers of the same service and, through that, available to or at risk of damage by unauthorised third parties. Independent audit and certification commissioned by the provider may provide that assurance.

Response:

Yes.

42. Will the service provider permit customers to undertake security testing (including penetration tests) to assess the efficacy of the access controls used to enforce the separation of customers' data?

Risk type	Control Category
Governance	Audit

Context:

If the provider does not provide access to independent audit reports and certifications, the agency should ensure that the provider permits customers to undertake their own security testing (including penetration tests). This should assess the efficacy of the access controls used to enforce the separation of customers' data.

Agencies may choose to assure themselves that access controls that separate their data from that of other customers are adequate. Even where an agency does not choose to at this point it may wish to retain the ability to do so at some future point. Where more than one public sector agency has data held in the same service, it may be financially prudent for them to work together so that a single assurance activity is undertaken that meets all their needs.

Response:

As per question 31, Sapient's SOC 2 Audit Report is available on request. Simply Energy will accept accredited third parties to perform penetration tests if customers require them, or it can nominate a third party to perform this upon request.

43. Does the service provider perform regular tests of its security processes and controls, including penetration testing?

Risk type	Control Category
Control of Information	Audit

Context:

Regular testing provides assurance that security controls and processes are operating effectively.

Response:

Yes, both Simply Energy and Sapient perform regular tests of their security, processes, and controls, including regular penetration testing by accredited third parties.

44. Does the provider supply customers with a copy of security testing reports?

Risk type	Control Category
Control of Information	Audit

Context:

Reviewing security testing reports provides the agency with an understanding of what has been tested and where risks may exist that require management.

Response:

Simply Energy will accept accredited third parties to perform penetration tests if customers require it. Alternatively, Simply Energy can nominate a third party to perform this upon request.

45. Is the service provider responsible for patching all components that make up the cloud service?

Risk type	Control Category
Service Continuity	Provider operations

Context:

A service provider may rely on a contracted third party to patch some components on which the agency's service is dependent. The provider needs to provide the agency with this information so that the agency can assess whether that results in any additional risk or exposure.

Response:

Patching for Simply Energy cloud services is managed by our Cloud Service Provider as a managed service.

Our third-party provider, Sapient, performs only patching across its development repositories and user vulnerability detection to determine where package patching is required.

46. Does the service provider's terms of service or SLA include service levels for patch and vulnerability management that includes a defined maximum exposure window?

Risk type	Control Category
Governance	Contract

Context:

Agencies need to be confident that vulnerabilities exposing their service or data to risk will be resolved promptly. This should include clear service expectations outlining how quickly a vulnerability will be addressed from first identification and how quickly a patch will be applied from first availability.

Response:

No, Simply Energy does not include SLAs for patch and vulnerability management. Simply Energy considers the Site iQ services a low-risk, non-business-critical platform, and SLAs for patch management should not be required.

47. Does the service provider allow its customers to perform regular vulnerability assessments?

Risk type	Control Category
Governance	Audit

Context:

Agencies may choose to perform vulnerability assessments to assure themselves of the security of the system delivering their service and holding their information. They may also choose to rely on vulnerability assessments undertaken by trusted third parties or work with other public service agencies to undertake assurance that meets all their needs.

Response:

Simply Energy will accept accredited third parties to perform vulnerability assessments if customers require it. Alternatively, Simply Energy can nominate a third party to perform this upon request.

48. Do the terms of service or SLA include a compensation clause for breaches caused by vulnerabilities in the service?

Risk type	Control Category
Governance	Contract

Context:

Breaches can result in significant costs to agencies. It's financially prudent for agencies to ensure that costs caused by the provider are borne by the provider.

Response:

No, Simply Energy does not include service or SLAs for compensation for breaches within agreements. Simply Energy considers the Site iQ services a low-risk, non-business-critical platform. As such, compensation for any loss of service has not been considered. Given the lack of personal or private information held on the platform, we refer to our standard terms and conditions for data loss or other breaches caused by vulnerabilities.

49. Does the cloud service enable the agency's service to be delivered using only approved encryption protocols and algorithms (as defined in the NZISM)?

Risk type	Control Category
Governance	Contract

Context:

NZISM defined a list of encryption approaches adequate for NZ Public Service services. The provider should, either by default or through configuration, allow the agency's service to be delivered using approved approaches.

Response:

Sapient and Site iQ uses TLS1.2 for data in transit and AES-256 encryption at rest.

50. Is it clear which party is responsible for managing the cryptographic keys?

Risk type	Control Category
Disclosure	Cryptographic

Context:

Responsibility for managing the cryptographic keys should be clearly defined and documented.

When relying on data encryption in the cloud service, the cryptographic keys used for the encryption are a critical asset. If cryptographic keys are lost or corrupted, then all the data encrypted with those keys may be unrecoverable. It's imperative that all parties understand their roles and responsibilities for managing those keys to prevent this from occurring.

Response:

Simply Energy and third-party Sapient are responsible for the encryption applied to Site iQ services. At this time there are no direct customer integrations that would require customer encryption.

51. Does the party responsible for managing the cryptographic keys have a key management plan that meets the requirements defined in the NZISM?

Risk type	Control Category
Disclosure	Cryptographic

Context:

Responsibility for managing the cryptographic keys should be clearly defined and documented.

When relying on data encryption in the cloud service, the cryptographic keys used for the encryption are a critical asset. If cryptographic keys are lost or corrupted, then all the data encrypted with those keys may be unrecoverable. It's imperative that all parties understand their roles and responsibilities for managing those keys to prevent this from occurring.

Response:

Yes, the solution uses TLS1.2 for data in transit and AES-256 encryption at rest.

52. Does the service provider and its subcontractors undertake appropriate pre-employment vetting for all staff that have access to customer data?

Risk type	Control Category
Governance	Provider operations

Context:

The service provider and its subcontractors should undertake appropriate pre-employment vetting for all staff who have access to customer data. Vetting should be repeated at regular intervals.

Many agencies require vetting for their own staff or contractors who have access to their information. Providers should be expected to have a process that is no less rigorous.

Response:

Yes, Simply Energy employees undertake pre-employment vetting as well as regular code of conduct refreshers to ensure staff comply with their obligations regarding security, privacy, compliance, and confidentiality. Job-specific training is provided as appropriate.

53 - Does the service provide logging that allows the agency to monitor user activity in the service?

Risk type	Control Category
Unauthorised access	Monitoring and Logging

Context:

Activity logging gives the agency visibility into what users are doing with the service. This is important for identifying and investigating unusual or suspicious activity, such as fraud or data breach.

Response:

Yes, user activity is monitored, and logs are stored indefinitely.

54. Does the service provider implement controls that ensure that audit logs are protected against unauthorised modification and deletion?

Risk type	Control Category
Governance	Provider operations

Context:

The service provider implements controls that ensure that audit logs are protected against unauthorised modification and deletion.

Audit logs are relied on for detection, investigation and prosecution of fraud and other inappropriate activity. It's important that audit logs are protected so that they can be trusted to contain an accurate and complete record.

Response:

Yes, access to logs and administration of logs are based on least privilege permissions.

56. Does the service provider have an SIEM service that logs and monitors activity within their environment and alerts unusual or inappropriate activity?

Risk type	Control Category
Unauthorised access	Monitoring and logging

Context:

The service provider should have an SIEM service that logs and monitors activity within their environment and alerts for unusual or inappropriate activity.

A SIEM provides the ability to automatically identify potential security incidents and assist with investigating incidents.

Response:

No, however, we do employ monitoring and alerting of access logs through AWS CloudWatch / CloudTrail.

57. Do the terms of service or SLA require the service provider to report unauthorised access to customer data by its employees?

Risk type	Control Category
Governance	Contract

Context:

Contract terms should require the service provider to report all identified unauthorised access to customer data.

Agencies have obligations for data in their control. These may include requirements to act or notify when information is accessed by an unauthorised party. These obligations may arise through different mechanisms including legislation (for example, the Privacy Act) or contract.

Response:

Yes, Simply Energy includes SLAs for unauthorised access breaches within customer agreements. It also has identity-based access (IAM) to all customer data platforms.

58. In case of unauthorised access to customer data is the service provider required to provide details about the incident to affected customers to enable them to assess and manage the associated impact?

Risk type	Control Category
Service Continuity	Contract

Context:

When unauthorised access is identified, the service provider should provide affected customers with details about the incident to enable them to assess and manage the associated impact.

Agencies have obligations for data in their control. These may include requirements to act or notify when information is accessed by an unauthorised party. These obligations may arise through different mechanisms including legislation (for example, the Privacy Act) or contract.

Response:

In the event of unauthorised access or a data breach due to situations outside of the customer's control, Simply Energy will notify and provide an incident report for assessment of impact and plan to perform the mitigated action within the agreed SLA timeframe.

59. Does the service provider have an auditable process for the secure sanitisation of storage media before it's made available to another customer?

Risk type	Control Category
Service Continuity	Contract

Context:

The service provider has an auditable process for securely sanitising storage media before it is made available to another customer.

For particularly high classification or sensitivity services, information agencies may require that when storage media is repurposed from holding that information, the storage media is sanitised. Where this is a requirement, the agency will need to be able to assure itself that sanitisation is occurring.

Response:

Simply Energy's technology assets are on Cloud platforms. Our terms and conditions with our managed cloud providers allow us to manage our security risks for disposing of data and assets securely.

60. Does the service provider have an auditable process for secure disposal or destruction of information and communications technology (ICT) equipment and storage media (for example, hard disk drives, backup tapes, etcetera) that contain customer data?

Risk type	Control Category
Data retention	Information management

Context:

If storage media cannot be sanitised, the service provider must have an auditable process for secure disposal or destruction of ICT equipment and storage media (for example, hard disk drives, backup tapes, etc.) that contain customer data.

For particularly high classification or sensitivity of services or information, agencies may require that when ICT equipment or storage media that has held that information is removed from use, it be securely disposed of or destroyed. Where this is a requirement, the agency will need to be able to assure itself that sanitisation is occurring.

Response:

Simply Energy and Sapient have robust services for data sanitisation, archiving and destruction where required. Simply Energy will disclose further information on these processes to customers if requested. Individuals have the right to request the deletion of their customer data under applicable data protection laws (e.g., GDPR).

61. Will the service provider allow the agency to review of a recent third-party audit report (for example, ISO 27001 or ISAE 3402 SOC 2 Type II) that includes an assessment of their physical security controls?

Risk type	Control Category
Unauthorised access	Audit

Context:

Agencies can reasonably expect that when they choose to rely on independent third-party assurance activities, they will be provided with sufficient information to understand the full scope and findings of those activities.

Response:

As per question 31, Sapient will provide their SOC 2 audit report on request.

62. If it's practical to do so (that is, the data centre is within New Zealand), can the service provider's physical security controls be directly reviewed or assessed by the agency?

Risk type	Control Category
Unauthorised access	Audit

Context:

Agencies may choose to assure themselves that physical security controls on access to data centres are adequate. Even if an agency does not want to do it now, it may want to retain the ability to obtain assurance in the future.

Where more than one public sector agency has data held in the same data centre, it may be financially prudent for them to work together to undertake a single assurance activity that meets all their needs.

Response:

Not applicable – all data centres are located outside of New Zealand.

63. Does the service provider provide data backup or archiving services as part of their standard service offering to protect against data loss or corruption?

Risk type	Control Category
Incident Recovery	Information Management

Context:

In some cases, the agency should consider having the service provider provide data backup or archiving service.

While providers may have in place many mechanisms to reduce the likelihood of data loss or corruption a separate backup would provide another level of mitigation. If the agency does not maintain a separate backup or archive, or if restoring data from a separate backup would take too long to meet the agency's needs, then the agency should consider procuring a backup or archival service from the provider.

Response:

Yes, raw data is archived indefinitely, processed and aggregated data is archived indefinitely, and Sapient platform data is backed up every hour. For Simply, backups are managed at least daily.

64. If a backup or archiving service is not included as part of their standard service offering, is it available as an additional service offering to protect against data loss and corruption?

Risk type	Control Category
Incident Recovery	Information Management

Context:

This service can be expected to incur an additional cost, so agencies may choose to consider whether other mechanisms are sufficient for the particular needs of the service and its data.

Response:

As per question 63, backup and archiving of the Site iQ services are Included as part of our standard service.

65. Is it clear how data backup and archiving services are provided?

Risk type	Control Category
Incident Recovery	Information Management

Context:

The agency should assess whether provided data backup and archiving services meet its needs.

If the agency chooses to purchase backup and archiving services, the provider should clearly explain how those services are provided so that the agency can assure itself that its needs are met and that the method introduces no additional risks (for example, another third party holding a copy of personally identifiable information).

Response:

Backup and archiving services are managed services as part of the Site iQ solution. Backups are managed in the following ways:

Data Warehousing

- Our data warehousing, which holds Site iQ data, has backup and archiving services, which our CSP provides as a managed service.
- Core systems associated with Site iQ have regular backup and archiving services. raw data is archived indefinitely, processed and aggregated data is archived indefinitely and is backed up every hour.

66. Does the SLA specify the data backup schedule?

Risk type	Control Category
Incident Recovery	Contract

Context:

Where backups are performed by the provider, the agency should agree on an acceptable backup schedule with the provider.

If the agency chooses to purchase backup and archiving services, the provider should be clear about the schedule of backups so that the agency can assure itself that its needs are met.

Response:

No SLAs related to backups or archiving are included in our service agreement.

67. Are the backups (whether performed by the service provider or the agency) encrypted using an NZISM-approved encryption algorithm and appropriate key length?

Risk type	Control Category
Disclosure	Cryptographic

Context:

Backups (whether performed by the service provider or the agency) are encrypted using an NZISM-approved encryption algorithm and appropriate key length.

Encryption of backups prevents them from inadvertently or deliberately exposing sensitive information.

Response:

Backups are encrypted using AES-256.

68. Is the level of granularity offered by the service provider for data restoration adequate?

Risk type	Control Category
Incident Recovery	Information Management

Context:

The agency should consider whether it might need to recover parts of a backup or whether a complete restoration of the full backup is sufficient.

Under some circumstances, an agency may wish to recover a small amount of data or a single item—a deleted client record or an overwritten document. If this is a necessary use case, the agency should confirm that the ability is supported by the cloud service.

Response:

Yes. Restoration from backups would be adequate to continue to provide service for customers.

69. Is the service provider's process for initiating a restore clear?

Risk type	Control Category
Incident Recovery	Information Management

Context:

The process for initiating a data restoration should be clear and understood by all parties.

If the agency chooses to purchase backup and archiving services, the provider should be clear about how the agency can initiate a data restoration. While some methods may be self-service and generate no additional cost, no outage, and no risk to services, others may result in the provider undertaking chargeable work and requiring a service outage. The agency should ensure that the process meets its needs and is adequately controlled.

Response:

Yes.

70. Does the service provider regularly perform test restores to ensure that data can be recovered from backup media?

Risk type	Control Category
Incident Recovery	Audit

Context:

The service provider should regularly perform test restores to ensure that data can be recovered from backup media.

By regularly performing test restores, the provider can provide assurance that the backup and restore process is effective.

Response:

Yes, tests are performed annually.

71. Does the SLA include an expected and minimum availability performance percentage over a clearly defined period?

Risk type	Control Category
Service continuity	Contract

Context:

Contract terms or schedules should include an expected and minimum availability performance percentage over a clearly defined period.

Availability may be affected by multiple factors, such as technical issues, faulty vendor hardware or software, facility issues (power loss) and deliberate attacks.

Response:

No, Simply Energy does not guarantee this as part of our standard agreement with customers. Site iQ is a low-risk, non-critical product, and this is considered not required.

72. Does the SLA include defined, scheduled outage windows?

Risk type	Control Category
Service continuity	Contract

Context:

Contract terms or schedules should include defined, scheduled outage windows.

Many agencies will prefer that they notify their own staff and customers of a regularly scheduled outage window.

Response:

No, SLAs are not included for outage windows. Site iQ is a low-risk, non-critical product with limited use outside of business hours. Where possible, Simply Energy will endeavour to ensure outage windows are maintained outside of operating hours.

73. Has the service provider implemented technologies that enable them to perform maintenance activities without the need for an outage?

Risk type	Control Category
Service continuity	Provider operations

Context:

If the service provider has implemented technologies that enable them to perform maintenance activities without an outage, then a defined, scheduled outage window may not be necessary.

Some agency services require high availability, and allowing for outages to enable the provider to perform maintenance may reduce the effectiveness and usefulness of the agency or its customers. Providers can implement solutions that decrease or eliminate these outages. This additional feature may be reflected in the price of the service, so for other agency services, this may not be a driver.

Response:

Yes, core systems related to Site iQ are largely serverless, so patching does not require downtime. The database technology is a highly available, multi-cluster managed service that does not require downtime for maintenance.

74. Does the SLA include a compensation clause for a breach of the guaranteed availability percentages?

Risk type	Control Category
Governance	Contract

Context:

The agency should include a compensation clause for a breach of the guaranteed availability percentages.

Failure to provide adequate availability of a service can result in significant costs to agencies. It's financially prudent for agencies to ensure that the provider bears costs caused by the provider.

Response:

No. There is no compensation clause for a breach of guaranteed availability. Site iQ is a low-risk, non-critical product. Whilst Simply Energy will strive to ensure the product has an update of as close to 100% as possible, there is relatively limited impact if the product is temporarily unavailable.

75. Does the service provider utilise protocols and technologies that can protect against Distributed Denial of Service (DDoS) attacks?

Risk type	Control Category
Service Continuity	Architectural

Context:

The service provider should utilise protocols and technologies that can protect against DDoS attacks.

Denial-of-service attacks are increasingly common and can affect the service's performance and availability. The provider may have options for preventing or limiting the impact of these attacks.

Response:

The solution uses load balancing and WAF to protect against DDoS attacks.

76. Can the agency specify or configure resource usage limits to protect against bill shock?

Risk type	Control Category
Uncontrolled cost	Configuration

Context:

The agency should be able to specify or configure resource usage limits.

If the service is billed according to resource usage, unexpected levels of use or malicious activity can escalate the cost. Setting usage limits allows the agency to control the maximum acceptable cost.

Response:

Site iQ is not billed according to resource usage. Unexpected increases in levels of use will not increase a customer's invoice. Site iQ pricing is agreed upon with the customer following site scoping and is a fixed fee per month, quarter, or year. This fee is derived based on the size of the customer's office and the amount of hardware installed on site. The agreed fee will remain for the length of the contract. Additional fees may apply if special services are requested by the customer. These types of services are specified in the service agreement.

77. Does the service provider have business continuity (BCPs) and disaster recovery (DCPs) plans?

Risk type	Control Category
Incident recovery	BCP and DCP

Context:

The service provider should have business continuity and disaster recovery plans.

The existence of appropriate business continuity and disaster recovery plans can provide some level of confidence that the provider is ready to respond to an incident. A provider without a plan is less likely to respond adequately. That said, the presence of a plan does not guarantee that the provider will execute the plan in a timely or effective manner.

Response:

Yes, both policies are in place and can be shared on request by both Simply Energy and Sapient.

78. Does the service provider permit the agency to review of its business continuity and disaster recovery plans?

Risk type	Control Category
Governance	Audit

Context:

The agency should consider reviewing the provider's business continuity and disaster recovery plans.

Agencies need to be confident that the provider's business continuity and disaster recovery plans are adequate for their needs and service and information. The plan needs to align with the agency's priorities, allow it to meet its obligations (including notification and communication with internal and external stakeholders), and allow the agency to be involved in decision-making when the decisions would be critical to the agency.

Response:

Yes, if requested, Simply Energy will disclose its business continuity and disaster recovery plans for Site iQ.

79. Do the service provider's plans cover the recovery of the agency data or only the restoration of the service?

Risk type	Control Category
Incident recovery	BCP and DCP

Context:

The service provider's incident recovery plans should ideally cover the recovery of the agency data. However, in many cases, the plans will only cover the restoration of the service.

Agencies need to be clear whether the provider will recover both the service and the agency's data or recover only the service and expect the agency to have itself kept a separate backup copy which can be copied into the provider's system.

Response:

Yes, recovery of data and restoration of service are covered in the standard Site iQ service.

81. Does the service provider formally test its business continuity and disaster recovery plans on a regular basis?

Risk type	Control Category
Incident recovery	BCP and DCP

Context:

The service provider should formally test its business continuity and disaster recovery plans on a regular basis.

By testing and refining its business continuity and disaster recovery plans, the provider can increase the likelihood that in an incident, its response will be timely and effective.

Response:

Yes, tests are conducted annually per the compliance policies.

82. Does the provider supply customers with a copy of the reports associated with the testing of business continuity and disaster recovery plans?

Risk type	Control Category

Incident recovery	Audit

Context:

The agency may choose to require that the provider supply a copy of the reports associated with the testing of business continuity and disaster recovery plans.

Agencies may wish to assure themselves by understanding the findings and recommendations of business continuity and disaster recovery plan tests. If they choose to request this, they should also request subsequent reports tracking the implementation of recommendations.

Response:

Yes, if requested, Simply Energy is willing to provide documentation supporting plans for business continuity and disaster recovery

83. Does the service provider have a formal incident response and management process and plans that clearly define how it detects and responds to information security incidents?

Risk type	Control Category
Incident recovery	Incident management

Context:

The service provider should have a formal incident response and management process and plans that clearly define how it detects and responds to information security incidents.

The existence of an appropriate incident response and management process can provide some level of confidence that the provider is ready to respond to an incident. A provider without a plan is less likely to respond adequately. That said, the presence of a plan does not guarantee that the provider will execute the plan in a timely or effective manner.

Response:

Yes. If requested, Simply Energy will disclose this incident response and management process to customers.

84. Is the agency able to review their incident management and response processes and plans to enable it to determine if they are sufficient?

Risk type	Control Category
Governance	Audit

Context:

For more critical services the agency may wish to review the provider's incident management and response processes and plans to enable it to determine if they will meet availability expectations.

Agencies need to be confident that the providers' incident management and response plans are adequate for the agency's needs service and information. The plan needs to align with the agency's priorities, allow it to meet its obligations (including notification and communication with internal and external stakeholders), and allow the agency to be involved in decision-making when the decisions would be critical to the agency.

Response:

As per workflow in question 83. If further information is required, please reach out to your Simply Energy point of contact.

85. Does the service provider regularly test and refine its incident response and management process and plans?

Risk type	Control Category
Incident recovery	Provider operations

Context:

The service provider should test and refine its incident response and management process and plans on a regular basis.

By testing and refining its incident management and response plans, the provider can increase the likelihood that in an incident, its response will be timely and effective.

Response:

Yes, processes are reviewed and adjusted every 2 years.

86. Does the service provider engage its customers when testing its incident response and management processes and plans?

Risk type	Control Category
Incident recovery	Incident Management

Context:

The provider may wish to engage the agency when testing its incident response and management processes and plans.

Agencies may wish to be involved in the testing of incident response and management plans where their service of information is highly critical or where they have concerns that the plan may not meet their specific needs.

Response:

No. While Simply Energy engages with third parties where required, it typically won't involve customers in this process.

87. Does the service provider provide its staff with appropriate training on incident response and management processes and plans?

Risk type	Control Category
Incident recovery	Incident Management

Context:

The provider may wish to engage the agency when testing its incident response and management processes and plans.

Response:

Yes, Simply Energy provides adequate training to its staff on incident response and management processes and plans.

88. Does the service provider's terms of service or SLA clearly define the support they will provide to the agency should an information security incident arise?

Risk type	Control Category
Incident recovery	Contract

Context:

Contract terms should clearly define the support the agency will receive should an information security incident arise.

The agency's ability to recover service after an incident may benefit from support from the service provider. However, this could increase the cost of the service, so the agency should consider its own incident recovery capability.

Response:

There are no standard SLAs for support required during an incident. Site iQ is a low-risk, non-critical product. Simply Energy will provide its best efforts to resolve any incidents that may occur; however, there are no SLAs unless terms are agreed upon between the customer and Simply Energy.

89. Does the contract require the provider to notify customers when an incident that may affect the security of their information or interconnected systems is detected or reported?

Risk type	Control Category
Incident recovery	Contract

Context:

The contract must require the provider to notify customers when an incident that may affect the security of their information or systems is detected or reported.

Agencies have obligations for data in their control. These may include requirements to act or notify when an incident affecting the security of their information occurs. These obligations may arise through different mechanisms including legislation (for example, the Privacy Act) or contract.

Response:

The agreement between Simply Energy and customers for Site iQ does not specify that customers must be notified during an incident; however, Simply Energy will always notify customers if an incident occurs where they have been impacted.

90. Does the contract specify a point of contact and channel for customers to report suspected information security incidents?

Risk type	Control Category
Incident recovery	Contract

Context:

The contract must specify a point of contact and channel for customers to report suspected information security incidents.

Agencies and affected parties must be able to contact the provider if they become concerned about a potential or actual security incident.

Response:

Yes, as per the service agreement, either party will notify the other party of a suspected security breach, and any such reports should be directed to your Account Lead or Site iQ representative.

91. Does the contract define the roles and responsibilities of each party during an information security incident?

Risk type	Control Category

Incident recovery	Contract

Context:

The contract should define the roles and responsibilities of each party during an information security incident.

Clarity of roles and responsibilities serves two purposes. First, it improves the likelihood that the incident will be handled appropriately and effectively. Secondly it allows the agency to be confident that it'll be able to discharge its own obligations and expectations.

The defined roles and responsibilities should cover the full breadth of incident response, for example:

- *who will brief the media or respond to media inquiries*
- *who will brief the Minister*
- *where an incident impacts more than one public service agency, the agencies should be able to work together to discharge their individual and collective obligations.*

Response:

No, the contract does not define the roles and responsibilities during an information security incident. Site iQ is a low-risk, non-critical product that predominantly holds plug load usage for commercial buildings. Very limited personal information can be exposed, and the value of the product is limited to the occupier of the commercial buildings.

92. Does the contract require that the provider provide customers with access to evidence (for example, time-stamped audit logs and/or forensic snapshots of virtual machines, etc.) to enable them to perform their own investigation of the incident?

Risk type	**Control Category**
Incident recovery	Contract

Context:

The contract should require the provider to supply customers with access to evidence (for example, time-stamped audit logs and/or forensic snapshots of virtual machines, etc.) to enable them to investigate the incident themselves.

Agencies may be required to or choose to perform their own investigation. To do so they will need access to information held by the provider or its own third-party providers. Where an incident impacts more than one public service agency, the agencies may work together to undertake a single investigation.

Response:

No, the contract does not specify that the provider provides further evidence of security incidents.

93. Does the provider share post-incident reports with affected customers to help them understand the cause of the incident and make an informed decision about whether to continue using the cloud service?

Risk type	Control Category
Governance	Contract

Context:

Does the provider share post-incident reports with affected customers to help them understand the cause of the incident and make an informed decision about whether to continue using the cloud service?

Agencies should be able to access post-incident reports to inform their own decision-making or to inform regulators or other third parties. Where an incident affected more than one customer and a single post-incident report was prepared, the agency will likely receive a copy that has been redacted to remove details of other customers' use or impacts.

Response:

Yes. Incident reports will be provided to affected customers to inform them of an incident, its cause, and its impact.

94. Does the contract and accompanying documentation provide sufficient information to enable the agency to cooperate effectively with an investigation by a regulatory body, such as the Privacy Commissioner or the Payment Card Industry Security Standards Council (PCI SSC)?

Risk type	Control Category
Compliance	Contract

Context:

Agencies may be required to or choose to enable a regulator or other third party to undertake an investigation. To do so, they will need access to information held by the provider or its own third-party providers. Where an incident impacts more than one public service agency, a single regulator or other third-party investigation may be undertaken.

Response:

Yes, this can be provided; however, it is worth noting that all Site iQ services are not subject to PCI requirements.

95. Does the contract specify limits and provisions for insurance, liability, and indemnity for information security incidents?

Risk type	Control Category
Uncontrolled cost	Contract

Context:

The agency should consider whether the contract should specify limits and provisions for insurance, liability and indemnity for information security incidents.

Security incidents can result in significant costs to agencies. It's financially prudent for agencies to ensure that costs caused by the provider are borne by the provider or their insurer. The agency should carefully review liability and indemnity clauses for exclusions.

Response:

Yes, as per clause 3, Liability – Exclusion and Limitation.