NEW ZEALAND CLOUD COMPUTING CODE OF PRACTICE

DRAFT FOR CONSULTATION

MARCH 2012 V1.1

New Zealand Cloud Computing Code of Practice.
Published by the New Zealand Computer Society Inc (NZCS) in March 2012.

NZCS
NEW ZEALAND COMPUTER SOCIETY

ADVANCING THE ICT PROFESSION

Table of contents

1 Introduction

The purpose of the New Zealand Cloud Computing Code of Practice ("The Code") is to enable professional cloud service providers to benchmark and demonstrate their practices, processes and ethics via a recognised third party to build trust with prospective customers. This can be achieved by service providers or suppliers meeting The Code, and having recognition made via a distinguished mark, or entry into a register of compliant cloud providers.

The Code assists end users by allowing them to make informed decisions based on the disclosure of practices of the service provider, enabling the end users to gain comfort with the service provider's ability to meet end users requirements.

The Code also builds trust within the Cloud Service Industry by providing a trusted format which both suppliers and customers can depend on.

Additionally service providers may wish to further their level of compliance by subscribing to an additional module of compliance. These modules provide a greater level of compliance in the areas of Security, Data Transportability, Service dependencies, and Business continuity, HR Procedures, Data Formats and Jurisdictions.

The code recognises the valuable financial support that the following organisations have made in order to have the Code of Practice developed, along with the participation of over 150 individuals from both around New Zealand and off shore.

NZCS NEW ZEALAND COMPUTER SOCIETY | ADVANCING THE ICT PROFESSION

Major Contributors

Equinox, Gen-i, OneNet, Webdrive, Xero, NZ Computer Society (NZCS).

Other Contributors

Salesforce.com, Google, EOSS Online Ltd, InternetNZ, NZRise, Systems Advisory Services.

1.1 Core Principles of the Code

The following are the Core Principles for the development of the Cloud Code of Practice. These Core Principles will continue to apply during subsequent development:

- **Not Re-inventing the Wheel**
  Where possible, the NZ Cloud Computing Code of Practice should leverage existing work in New Zealand and abroad and give clear preference to established prior work over creation.

- **Consistency with Global Practice and Structure**
  A core part of this initiative is researching approaches taken to addressing the core issues in overseas jurisdictions, to ensure the result is consistent with practices in other countries.

- **Research based on arbitrary approach**
  The recommendations and resultant Code will be developed based on demonstrable good practice and decisions taken based on sound research-based principles.

- **Facilitation of Development with Wide consultation**
  The role of NZCS and the project team is to facilitate the development of the code in consultation with as broad a range of stakeholders as possible and practical.

- **Preference for consensus based result**
  The project team will work towards a consensus view in terms of the structure and content of the Code. While consensus does not mean unanimous, the intention is to gain the wide support of a broad range of stakeholders.

- **Clear separation between governance of process and development of the Code**
  The steering group will govern the process, ensure the principles are adhered to and test the evidence based approach, however will not guide or influence the final result and code.

- **Compliance and Assessment**
  It is not the intention of the exercise to place undue or unnecessary compliance costs or processes on those that may wish to adhere to the code once developed, over and above what is necessary for the integrity of the code.

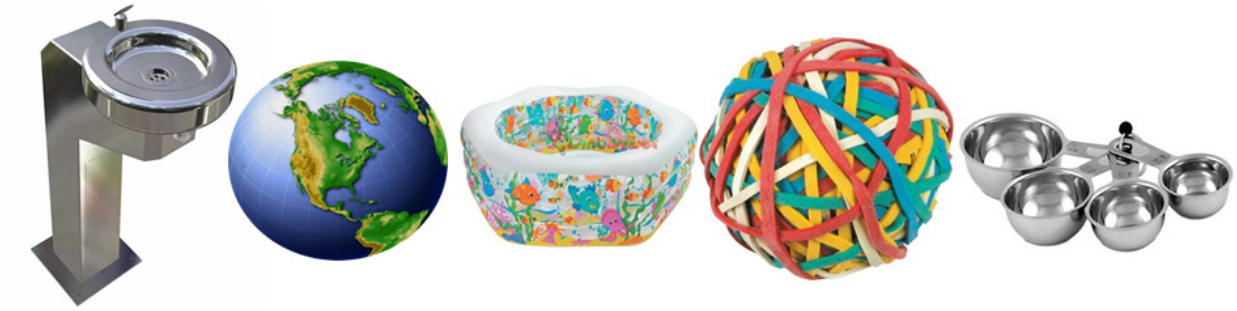
1.2 Aims of the Code

The Code aims to:

- Improve the standard of services being provided by New Zealand Business in the Cloud Computing Industry
- Set a standard of disclosure within the industry
- Create openness between suppliers and customers with regards to data protection, sovereignty and privacy
- To strengthen the integrity of Cloud Computing in New Zealand.

2 Defining Cloud

5 Essential Characteristics of Cloud Computing



On-demand self-service | Ubiquitous network access | Location transparent resource pooling | Rapid elasticity | Measured service with pay per use

Source: http://aka.ms/532

Cloud Computing has many definitions worldwide and certainly means many different things to many different people. The National Institute of Science and Technology (NIST) have created a definition, which is the most adapted definition in use today. NIST Identify five essential characteristics for cloud computing as illustrated above.

For the purpose of this code of practice we have simplified the NIST definition to ensure a simple definition that is easily understood, while formally supporting the full NIST definition as the authoritative definition of Cloud Computing.

Full NIST Definition: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

2.1 What is Cloud computing?

For the purpose of the New Zealand Cloud Code of Practice, Cloud computing is to be defined as:

"On-demand scalable resources which are provided as a service such as networks, servers and applications, that are accessible by the end user and can be rapidly provisioned and released with minimal effort or service provider interaction".

3 Application

3.1 Who does this Code of Practice apply to?

The New Zealand Cloud Computing Code of Practice applies to businesses who offer remotely hosted IT services of any type, either from New Zealand or within New Zealand, that meet the definition of Cloud Computing as outlined above.

The New Zealand Cloud Computing Code of Practice does not in any way place legal obligations on any of the parties participating in the Code, however any participant knowingly falsifying information will be subject to consequence under New Zealand law.

4 Approach

4.1 Cloud Code of Practice to relate to Provider's Products or Services

The Code will relate to the products or services offered by Cloud providers. This means:

- Providers whose offerings meet the test of compliance stated in Clause 4.2 may state that they are compliant with the NZ CloudCode
- The product to which the disclosure statements apply under this code of practice must be described in Clause 5.2 of this document.

4.2 Compliance with the Code of Practice

The Code is a voluntary code. Those who are formally compliant to this code will:

- Comply with the code's minimum level of security requirements as described in clause 5.4
- Adhere to the code's good practice guidelines
- Have available a full and complete set of of the disclosures prescribed in the Code to all existing and potential clients at all times
- Proactively provide a list of these disclosures to all prospective clients
- Update information as disclosed to their clients prior to a change being made or if this is not possible, within 28 days at most of such a change to disclosures
- Maintain a professional service to their clients
- Provide a link to their disclosure statements on their publicly available website
- Promote the Cloud Code of Practice on their site via a link to the NZ Cloud Code website
- NOT market a product or service as a "Cloud" product or service unless it meets the cloud definition as above
- NOT market a product or service as a "Cloud" product unless it meets all base requirements of the Code
- Undertake any formal assessment or review as determined from time to time by the organisation responsible for the operation of the Code and pay any prescribed fee
- Be registered on a publicly available *Register of Compliant Cloud Providers*.

Organisations that become compliant to this code may also choose to subscribe to additional modules of the code, providing more detail and protection for the end users, and using more detailed levels of best practice in their service offering.

5 Code of Practice Disclosures

5.1 Disclosure

For an organisation to be compliant with this code they must truthfully disclose the following information to all clients, both prospective and current, before, during and after the sales process. They are required to update any disclosures and actively inform clients of these changed disclosures as soon as possible and not later than 28 days of that change being made.

The applying organisation must comply with each of these requirements. An organisation may choose to subscribe to additional disclosure modules highlighting their further commitment to their standards of good practice.

The standard areas of disclosure required by this code are:

5.2 Corporate Identity

Knowing who you are doing business with and how to contact them is an important part of building trust.

Company name: .....

Trading name: .....

Physical address: .....

Postal address: .....

Contact phone number: .....

Contact email address: .....

Contact person responsible for these disclosure statements: .....

The disclosures herein apply to the following products supplied by us:

- .....
- .....
- .....
- .....

5.3 Ownership of Data

The ownership of data supplied by the client to the service provider needs to be clearly disclosed. This section helps identify who owns client data, and data generated by the service provision.

- Data uploaded to our service is deemed to be owned by the **client**/**service provider**/**other**
- The upstream providers that we use considers the data that you use or transmit via our service as owned by **client**/**service provider**/**upstream provider**
- Meta data and other statistical information generated as a result of the use of our service is owned by **client**/**service provider**/**other** and **is**/**maybe** used for the purposes of ……

5.4 Security

Ensuring that a cloud service provider has a good set of standards and practice surrounding security is imperative. For this reason, the Cloud Security Alliance STAR registry (https://cloudsecurityalliance.org/star/) has been selected as the minimum standard. Cloud Service providers who are currently undergoing the process of being added to the STAR registry will be given a pending status to their compliance to the code and are expected to have completed the process within 30 days.

- As at the date of application: *(select the statement that applies)*

  'We are currently undergoing the process of aquiring the Cloud Security Alliance STAR registration'

  Or

  'We currently are registered on the Cloud Security Alliance STAR registry'.

5.5 Data Location

Services providers may host data on a number of services, located locally or offshore, knowing where hosted data is located can help customers assess any risks or benefits for their business.

- Our Primary systems that host your data are located in …… *(state country)*
- Our **Backup**/**Disaster** recovery systems that hold your data are located in …… *(state country)*
- Data is housed on servers located in …… *(state country)*, with **backup**/**archived data** being located in …… *(state country)*.

Additional disclosures may be provided here by the service provider such as the location of specific data centres and backups.

5.6 Data Access

Knowing how customer data can be accessed both during and after a service has been provided is an important step to ensuring that, when a service has been ceased, the right provisions are made.

- Your data may be accessed during the contract period as described in our contract with you
- At the cessation of our service to you, your data **will**/**will not** be available to access

  - (if answer above is "will be available") Access to this data will be possible via …… *(state method)*

  - There **will**/**will not** be additional charges for access of your data after the service has been ceased.

5.7 Back up and maintenance

Understanding the backup procedures of your service provider and their maintenance policies allows the customer to make decisions on what further steps they may need to ensure their data is backed up sufficiently.

- Backups are performed every …… *(how often – hourly, daily, weekly, monthly)*
- Backups start at …… *(start time)* and finish at …… *(finish time)*
- Backup data is stored …… *(onsite, or offsite, relative to the location of the data being backed up)*
- Where backup data is stored offsite, the offsite location is …… km *(minimum kilometres distant from the location of the data being backed up)*
- We test the restoration of backup data every …… *(how often)*
- Access to backup data or archive data **is** / **is not** available via …… *(method)* ……
- Adhoc requests for restoration of customer data will be completed within …… *(elapsed time from request)*
- We **do** / **do not** allow client audits of backup data, costs of which will be carried by ……
- Back up data is retained for …… *(state period)*
- We **do** / **do not** undertake a regular maintenance programme to ensure the reliability and stability of our service
- We **do** / **do not** archive data separately to back up data.

Note: Backups should not be limited to 'customer data'. They must also include any data or configuration items which form 'the service' being provided by the cloud service provider, including (where applicable), but not limited to: customer data, configuration settings, files, documents, operating systems, applications, permissions. The Backup and Subsequent Restoration capability must be comprehensive enough to enable the CSP to fully restore-to-operation the 'Service' and any customer data.

5.8 Geographic Diversity

It is likely that a service provider may provide services from multiple locations in order to provide resilience of service when adverse events affect one of the locations. This section seeks to understand the locations in which the service provider provides services from and carries out their business.

- Our service **is** / **is not** provided via multiple locations *(if the service is provided via multiple locations the following disclosures should be made)*
  - Our services **are** / **are not** more than 150km apart in distance
- Our services are provided from the following locations …… *(stating the cities and countries where services are being provided from)*
- We operate offices in the following cities ……

5.9 SLA and Support

Service providers may offer premium support packages that are additional to their standard service offering; likewise your contract with them may have special support services just for you. This section sets out the **standard** support mechanisms and service level agreements that apply to their services.

- Our standard support hours are .....
- The following time zones apply to our support hours .....
- Our Service uptime over the previous 12 months has been .....
- In the event of an unscheduled outage or incident, we will communicate the details of the issues and expected resolution times via .....
- When communicating an issue to us we prefer you to do so via .....
- Our standard response time to any issue raised is .....
- In the event of a major incident, we will update our notifications every ..... hours
- When communicating with you we will use ..... *(e.g. details provided by customer on application)*
- We **do**/**do not** make incident reports available to our clients after a major incident
- We operate and **active**/**active**, **active**/**passive**, **or other** based service
- We classify incidents and therefore the resolution time to issues in the following way:

Severity Level	Classification Method	Expected resolution time
e.g. Major	e.g. affects more than 70% of clients during business hours	4 hours
e.g. Critical	e.g. affects more than 50% of clients during business hours	4 hours
e.g. Minor	e.g. affects less than 10% of clients outside of business hours	6 hours

Additional "plain english" statements may be offered under this heading with regards to the service providers service and SLAs.

5.10 Privacy Policy

It is important that the customer is aware of what policies are in place surrounding the use of client data by the service provider along with issues such as access to that information, law enforcement action and breach policies. This section attempts to clarify these points and more relating to privacy issues.

- You can access the data we hold via …… *(state method)*
- We use our customer data for business functions such as ……
- *Deletion of all* customer data at the cessation of our service to you takes place …… *(state timeframe)*
- It is our policy to provide information to law enforcement agencies when presented with a valid court order
- There may be times when we are approached by various law enforcement agencies informally requesting access to certain customer data, it is our policy **to**/**not to** co-operate with law enforcement agencies in these instances
- In the event of a loss of data, we will provide information to you via …… *(state method)* as soon as practicable
- In the course of providing services to you, we **do not**/**may** need to access your data for purposes integral to the delivery of or remedy of the service we provide
- The access of your data may be for the following purposes. ……
- We **do**/**do not** make further use of data provided to us for commercial gain
  - The use of data is of the following nature ……

6 Additional Modules

Cloud Providers may subscribe to the following additional models should they wish to promote a higher level of compliance to their clients.

6.1 Enhanced security

Service Providers, who have certified external standards (such as CSA's CCSK, a relevant ISO standard or similar) which are recognised on the *Schedule of Enhanced Security Certifications* released with the Code from time to time, may provide details of these certifications here.

6.2 Data Transportability

This section identifies how data may be obtained during the service being provided and after the service has ceased and any related costs.

- We **allow**/**do not allow** the use of an API to access data during the service provision
- Your data can be downloaded from our service during the service provision via the following formats ……
- Data **will**/**will not** be available to download after we cease supplying service to you *(if data is available post service cessation, then the following statement will apply)*
  - Data can be obtained via ……
- There **will**/**may**/**will not** be additional charges associated with accessing data after your service has ceased.

6.3 Service Dependencies and Business Continuity

The service provider should disclose any service dependencies they may have, such as upstream providers and what their own Business Continuity preparations are, which may include an upstream providers SLA, redundancy and failover.

6.4 HR/Personnel procedures

This section seeks to understand the HR processes to ascertain suitability of qualified staff.

- We **do**/**do not** undertake pre-employment checks including police and or security checks
- We **do**/**do not** provide a regular formal in-house training program for technical staff
- We **do**/**do not** have a requirement of formal qualifications of key technical staff
- We **do**/**do not** have a confidentiality policy that all staff must adhere to
- We **do**/**do not** engage external providers to deliver training programs to staff.

6.5 Data Formats

- Data uploaded to our service is deemed to be owned by the **client / service provider / other**
- The upstream providers that we use considers the data that you use or transmit via our service as owned by **client / service provider / upstream provider**
- Metadata and other statistical information generated as a result of the use of our service is owned by **client / service provider / other** and **is / maybe** used for the purposes of .....

6.6 Jurisdictions

- For the purpose of Legal Jurisdiction, the contracted supplier who provides the service to you is a company registered in ..... *(state country)*
- The Governing law of our contract with you is ..... *(state jurisdiction)*.

6.7 Ownership of Application

- The source code for the applications that you use on our service **is / is not** available to license outside of our service provision
- It **will not / will** be possible to use your data outside of our service (i.e. your local network) by ..... *(state details of how the application can be run outside of the service providers systems)*.

7 Customer Engagement

Good practice dictates that a provider should be explicit about the right to audit inside their contracts, stating who will perform the audit, who pays for the audit, what information you will receive and what it means.

As participants in the NZ Cloud Code of practice, we confirm that we act lawfully within the Privacy Act, Fairtrading Act, Commerce Act and other relevant legislations.

- We **do / do not** have a current Fair Trading Act Compliance policy
- Complaints about our service can be made in the first instance to ..... *(contact details of the relevant contact point for complaint handling inside the organisation)*.

8 Assessment

This section should outline how compliance with the code is assessed and who by and at what frequency. The full details of this section are outside the scope of this part of the project.

9 Recognition of Compliance to this code

Organisations that are compliant with the Code will be authorised to use a code of practice compliance logo on their marketing and website (which must link back to the Code website).

The Code will also specify specific wording that can be used in marketing collateral, tender responses and quotes. Promotion of the Code will be restricted to specific wording to ensure consistency, clarity in terms of what this means and providing uniformity in the way the Code is promoted to the public.

10 Maintenance of this code

This section will detail how this code will be maintained, by whom and how often. It will also offer a complaints resolution procedure for dealing with claims that a provider is not complying with the Code (following unsatisfactory internal resolution). The full details of this section are outside the scope of this part of the project.

Schedule 1:
Fair trading compliance policy

Fair trading compliance policy (sample)

The following text can be used to create a compliant Fair Trading Compliance policy.

PURPOSE

1. The purpose of this policy is to ensure that:
   - all advertising and marketing used by *[insert name of business]* will comply with New Zealand's Fair Trading Act 1986; and
   - the advertising or marketing materials that we use and the associated activities we undertake will not (and could not) mislead or deceive our consumers.

SCOPE

2. This policy relates to all the things we say and do about the promotion and sale of the products and / or services we supply to consumers. This includes sales techniques and financing as well as advertising and marketing using print materials, broadcast advertising, electronic advertising, verbal messages and other forms of promotion.

WHY WE HAVE THIS POLICY

3. Consumers come from a wide range of social, cultural and educational backgrounds. Because of this, we need to be clear about the things we say and in doing so we reduce the risk of consumers misinterpreting our intentions or of us misleading them and therefore potentially breaching the Fair Trading Act.
4. The benefits for *[insert name of business]* having in place a Fair Trading Act policy and compliance programme include:
   - having better informed staff and improved customer service;
   - having better customer relations;
   - enhancing our business culture; and
   - maintaining and enhancing our good reputation.

RULES AND RESPONSIBILITIES

5. All advertising and related activities will be truthful and only contain statements and visual representations which ensure an overall impression that:
6. **does not** and is not likely to mislead or deceive consumers;
7. **does not** make false and misleading representations; and
8. **does not** abuse the trust of the consumer or exploit their lack of experience or knowledge.
9. All staff with trading / sales responsibilities must be informed of this policy and know how it applies to the work they do.

Managers are responsible for ensuring that their staff with trading / sales responsibilities are aware of all current promotions and advertising (representations) being made about the products and / or services that they supply.

All staff are responsible for immediately notifying suspected breaches of this policy to *[insert management / the person responsible for the promotion / advertising]*.

All staff with trading responsibilities will receive regular Fair Trading Act compliance training. Records of training must be maintained.

10. Initial Fair Trading Act induction training will cover:
    - awareness of this policy;
    - the responsibilities of staff and management relating to Fair Trading Act compliance; activities;
    - what is a false or misleading representation; and
    - what to do if a breach of this policy occurs.
11. *[insert name of position or person]* will be responsible for the education and compliance activities associated with this policy and the Fair Trading Act.
12. All marketing decisions and strategies will be reviewed by management to ensure they meet the requirements of this policy.
13. Product managers (or others with product management responsibilities) are responsible for ensuring that all advertising is fit for purpose and checked for compliance with this policy **before** it is cleared for use.
14. An in-house system for checking and approving all publicity material against the requirements of this policy and the Fair Trading Act will be used by relevant staff, managers, contractors and advertising agencies (refer to Check Sheet 1: Fair Trading Act advertising / promotion compliance).
15. The person who checks the material should have reasonable product knowledge about the products and / or services being promoted. The person who then approves the material must have the authority to approve advertising representations in *[insert name of business]*.
16. The Fair Trading Act complaints register will be used by *[insert name of business]*.
17. All Fair Trading Act complaints made by consumers and competitors will be:
    - recorded in a complaints register;
    - managed promptly to ensure any potential breaches are rectified immediately and suitable action(s) put in place to reduce the likelihood of reoccurrence; and
    - reported periodically to *[insert senior management / the Board / other]*.
18. Any mistakes in published advertising materials will be remedied immediately, including destroying or carefully altering the advertising materials and alerting consumers to the error. As appropriate, managers should be assigned to handle any dissatisfied consumers.
19. Out of date advertising materials will longer be displayed or used in promotions.

BASICS ABOUT THE FAIR TRADING ACT

20. The following information covers the basics about the Fair Trading Act. The Act:

    - prohibits people in trade from engaging in misleading or deceptive conduct generally;
    - prohibits certain types of false or misleading representations about goods or services (e.g. false claims about skills, qualifications, success, test and survey results);
    - prohibits certain types of false or misleading representations or conduct in relation to land;
    - prohibits certain unfair trading practices (i.e. bait advertising, offering gifts as part of a promotion with no intention of supplying them or misrepresenting the nature of the gift, using packaging that misrepresents the products inside);
    - provides for consumer information and product safety standards regulations and unsafe goods notices; and
    - prohibits misleading conduct in relation to employment offers.

21. The Ministry of Consumer Affairs is responsible for administering the Fair Trading Act, including reporting to Government on the need for changes to the current law and other policy matters. The Minister also has the power to order compulsory recall of goods which fail to meet a product safety standard or which may cause injury.

22. The Commerce Commission is responsible for enforcing the Fair Trading Act. In taking action against a business that may have breached the Act, the Commerce Commission's focus is not on whether *[insert name of business]* ever intended to deceive or mislead consumers, but whether the things we have said and done are liable, or likely, to deceive or mislead consumers.

DEFINITIONS AND EXAMPLES

Advertising	Any form of communication made to the public or a section of the public for the purpose of promoting the supply of products or services or the sale of property. Examples include: • broadcast advertising. This can include television and radio advertising and infomercials; • electronic advertising. This can include website, text messages and email; • print materials. This can include product labelling, guarantees, pledges, mailers, flyers, newspapers, brochures, magazine and journal advertisements, billboards, point-of-sale and other display material; and • verbal messages. This can include sales pitches, promises and general product and service information provided verbally in person or by phone.
Complaints handling system	A customer feedback system for collecting and recording complaints about our Fair Trading Act compliance activities. An effective complaints handling system enables us to properly manage each complaint and learn and improve on what we do.
Deceive	To cause to believe what is false, to mislead as to a matter of fact, to lead into error; to delude, take in.
Mislead	To lead astray in action or conduct, to lead into error, to cause to err.
Representation	A representation is any factual statement made about a product or service, either orally or in writing. A representation may also be an impression given by pictures, advertisements, promotional material or a sales pitch, by general conduct, including by keeping silent when critical information should be given. Representations can also be made in specifications and product descriptions, warranties and contracts.
Supply	For products, supply can include supply by gift, sale, exchanges, lease, hire or hire purchase. For services, supply can include the providing or giving of a service.
Trade	Any trade, business, industry, profession, occupation, activity of commerce or undertaking relating to the supply or getting of products or services or land. Few undertakings, except one-off private transactions, escape the jurisdiction of the Fair Trading Act.

INFORMATION SOURCES

23. More information about the Fair Trading Act and achieving compliance with the Act can be obtained from the following sources:

    - The Fair Trading Act 1986 www.legislation.govt.nz
    - Ministry of Consumer Affairs www.consumeraffairs.govt.nz
    - Commerce Commission www.comcom.govt.nz
    - The Advertising Standards Authority www.asa.co.nz

This policy is authorised by:

....

Name and position *Date*

Disclaimer

These compliance resources are guides only and reflect the Commerce Commission's view. Use of these compliance resources does not in itself guarantee compliance with the Act. However, an effective compliance programme, properly implemented, should mitigate the risk of contravening the Act.

Only the courts can make an authoritative ruling on breaches of the Fair Trading Act. These compliance resources are not intended to be definitive and should not be used instead of legal advice.

Schedule 2:
Cloud Security Alliance STAR Registry Information

The CSA Security, Trust & Assurance Registry (STAR) is a publicly accessible registry that documents the security controls provided by various cloud computing offerings, thereby helping users assess the security of cloud providers they currently use or are considering contracting with.

The CSA STAR service is based upon the CSA Governance, Risk and Compliance (GRC) Stack, a collection of four integrated research projects that provide a framework for cloud-specific security controls, assessment, and greater automation and realtime GRC management.

There are two self assessment models inside the STAR program, the Cloud Controls Matrix (CCM) and the Consensus Assessments Initiative Questionnaire (CAIQ, pronounced cake) Service Providers can choose which model to undertake.

The Cloud Controls Matrix (CCM), provides a controls framework that gives detailed understanding of security concepts and principles that are aligned to the Cloud Security Alliance guidance in 13 domains. As a framework, the CSA CCM provides organizations with the needed structure, detail and clarity relating to information security tailored to the cloud industry. Providers may choose to submit a report documenting compliance with Cloud Controls Matrix.

The Consensus Assessments Initiative Questionnaire is based upon CCM and provides industry-accepted ways to document which CCM security controls exist in IaaS, PaaS, and SaaS offerings. The questionnaire (CAIQ) provides a set of over 140 questions a cloud consumer and cloud auditor may wish to ask of a cloud provider. Providers may opt to submit a completed CAIQ, this will likely be the easiest option for those who have not already developed a CCM report.

More information on the CSA STAR registry can be found on the Cloud Security Alliance website here: https://cloudsecurityalliance.org/star/