New Zealand Cloud Computing Code of Practice

Formal Submission Public Report
March 2012 v1.0

Contents

Introduction

The Development of the New Zealand Cloud Computing Code of Practice is the result of an industry wide call for standards to be set to help protect the reputation of those providing professional services within the cloud computing industry, as well as to help define what good practice should look like in New Zealand.

NZCS was asked to independently facilitate the first part of this process, being the creation of the code, which has been funded by industry on behalf of the ICT community in New Zealand. NZCS is a fully independent organisation without allegiance to any particular vendor or vendors and has experience in creating code of practice and other related documents.

The initial phase of the exercise is to determine, in detail what the code of practice will look like, specifically what level of complexity and detail should be incorporated into the code.

To achieve this, wide consultation with stakeholders such as cloud suppliers, consultants and cloud customers was undertaken, via 6 workshops held in Auckland, Wellington and Christchurch, along with one nationwide video conference. The workshops were attended by over 150 people from all types of businesses, from small NZ businesses through to large multinational organisations.

After the workshops were held a survey was sent to the attendees of the workshops and others who had joined the Reference Group, the submissions made by the 78 respondents to that survey are the basis of the NZ Cloud Computing Code of Practice Draft Structure document.

Formal feedback on the NZ Cloud Computing Code of Practice Draft Structure document was called for between 23rd December 2011 and 1 February 2012. This document collates the submissions received into each of the areas that feedback was sought on, and provides the basis for the change document which provides information on the changes made to the draft document to transition it to the NZ Cloud Code Skeleton Document

1. Respondents

To allow for some understanding of the perspective that these submissions have been made with, the following table shows a general description for each.

Respondent Number	Description
1	Large multinational primarily based outside of NZ
2	Small - Medium sized NZ based provider
3	Large multinational primarily based outside of NZ
4	Small -Medium sized NZ based provider
5	Large NZ based provider
6	Large National organisation – Customer
7	Interested Individual
8	Small -Medium sized NZ based provider
9	Interested Individual
10	NZ Based independent Consultant
11	NZ Based independent Consultant
12	Interested Individual
13	SUBMISSIONS REMOVED AS PER REQUEST
14	Small -Medium sized NZ based provider
15	Industry Group
16	Small -Medium sized NZ based provider
17	Government Office

3. Areas of Consultation

This round of consultation was limited to the structure, approach and scope of the New Zealand Cloud Computing Code of Practice only and feedback on specific areas was sought. Below are the submissions received on each of those areas.

While most submitters followed the consultation document and provided responses accordingly, some did not. Respondents details have been removed, however each submission has been numbered for reference, and those numbers are included below.

Some submissions have been edited, removing open questions or commentary regarding content of the code which is not covered in this stage of feedback. Comments directly pertaining to the content of the code have been forward to the relevant groups responsible for developing the content in each specific area.

1. Definition of Cloud Computing

The draft document uses an adapted version of the NIST definition for the purpose of the code of practice for simplification purposes but refers to the full NIST definition as the authoritative definition.

Do you agree with this approach, if not – what suggestions can you make to define cloud for the purpose of this code of practice?

Responses

Respondent #	Submission
1	We agree with this definition
2	Agreed
3	No Response
4	The difficulty in providing a definition means that there will be many loop-holes left for unscrupulous operators to find a way through. A more general description including the processing and retention of data belonging to a third party will likely provide more protection for users. We note that on-line storage (storage-as-a-service) is excluded from the definition, which is an omission
5	Perhaps a list of bulleted understandable explanations of the 5 measures of cloud in there (with examples) so laymen can understand this easily
6	No Response
7	No Response
8	I propose that the definition of cloud be amended slightly to take into account service providers who offer virtual private clouds not immediately available by the internet. To achieve this, consider changing “the internet” to “public or private networks”
9	No Response
10	....One draft definition I saw used the word “internet” and while I agree this is likely to be the most common delivery vehicle for cloud computing services it is not the only possibility. The NIST model works well for me. .....There is enough confusion as to what Cloud computing is already. Simplifying the definition is likely to allow that confusion to propagate. While the NIST definition complete with the list of essential characteristics, Service Models and Deployment Models is long-winded it is fairly comprehensive. I believe that Cloud Computing cannot be accurately defined succinctly in a nutshell. If people really want to understand what cloud computing is they need to take time to read the full NIST definition
11	No Response
12	I Agree with the approach outlined
13	SUBMISSION REMOVED
14	No response
15	No response

16	The definition still says “accessible via the internet” which excludes private clouds from the Code of Practice. It would be better to say “accessible via internet based technologies” (in the sense of IP Based networks), as it will cover well all forms of Cloud Computing.
17	We have no particular comment to make on the definition itself.

2. Application of the code

We have defined who the code of practice should apply to with the following statement:

“… businesses who operate within New Zealand that offer remotely hosted IT services of any type that meet the Cloud Code definition of Cloud Computing.”

Do you agree this is the best way to represent the Cloud computing industry and the wide range of services it may cover both now and in the future, while also distinguishing “proper” cloud offerings from those that use the term to market generic products?

Responses

Respondent #	Submission
1	We agree with the scope of the application of the Code and note that the term “operate” should not necessarily mean the provider must have a registered company or business in New Zealand, but just that it offers services to customers in New Zealand
2	It is not clear what “operate within New Zealand” means. Does it include businesss with no NZ Presence but who offer services to NZ based customers? Or is it only NZ Based businesses.....
3	No Response
4	This is correct. There is clear definition between an internal cloud (behind the firms firewall) and external clouds run by third parties. It does not make sense to treat both internal and external clouds in an identical manner
5	No Response
6	No Response
7	No Response
8	No Response
9	No Response
10	Agree. Some services providers may try to exclude themselves from the Code of Practice by stating that they do not offer cloud computing services when they actually do. Given the popularity of the Cloud “brand”, I think this is unlikely
11	No Response
12	I agree with the definition of business to which the code complies, I agree that there needs to be a distinction between “proper” cloud offerings versus more generic products and the definition as per the draft document captures it succinctly
13	SUBMISSION REMOVED

14	No Response
15	No Response
16	No Response
17	No Response

3. Approach and Compliance

The New Zealand Cloud Computing Code of Practice is an Industry led voluntary code. As highlighted in the Structure and Approach Survey Document, 73% of survey respondents preferred a disclosure based code. Over 50% of all respondents wanted some form of assessment, whether it be random, complaints based or the basis of compliance under this code.

The draft structure and approach document suggests that initially the code should be disclosure based with a modular option available to suppliers, to allow for initial flexibility in the codes infancy, providing a foundation for further evolutions in the code progressing to a multi-tiered approach in the future as the industry and code matures.

Do you agree with this approach? Do you feel that the code should perhaps initially start with a multi-tiered structure? Do you agree that a disclosures based code of practice is suitable for the New Zealand industry? What are your thoughts on a self assessed code and the practical application of this.

Responses

Respondent #	Submission
1	We agree with the approach in Principle. We do not agree that the code should commence with the multi-tiered structure and instead that the more detailed modules should be developed once it is clearer who the code is being used and perceived. We agree that a disclosure based code makes sense for the NZ industry.... We do not agree that providers must provide the disclosures statement to every customer upfront. This will be unworkable to those providers whose customers self-provision on the web and there will be no contact with the customer.... Hosting the disclosures on the provider’s website should be sufficient... We also do not agree that a misleading and deceptive conduct statement is necessary and is not within the scope of the code.

2	...does not agree that the compliance should relate to all cloud products. There does nt appear to be a sound reason why compliance cannot be achieved in relation to some or most products provided which products are covered is entirely clear. This is particularly key for resellers and consultants who may not have all the information required to achieve compliance for every product. A disclosure based code is appropriate. Although a self assessed code is open to abuse by those claiming compliance without actually achieving it, the costs of some form of audit would likely outweigh any benefits. Requiring specific disclosures means that the code may need to be regularly updated to keep pace with a rapidly changing industry. Need for flexibility and likelihood of change should be taken into account when determining what those disclosures should be (e.g. in relation to security)
3	...is in favor of a voluntary, self assessed Code, using general principles to determine its disclosure requirements. The requirements in paragraph 4.2 of the Draft Structure and Approach for vendors to display certain information on their public websites are difficult to implement for global vendors and in our view unnecessary. Specifically, the requirements to promote the code with a link to the NZ Cloud Code website and a link to disclosure statements featuring prominently on the website of the provider. As a global cloud provider, if [name removed] complies with the code it will want to tell prospective customers in New Zealand however it would be challenging to change [name removed]'s global terms and conditions or product web pages. Recommendation: A more suitable solution would be to require vendors who claim to comply with the code to produce a statement of compliance on demand for prospective customers. The organisation with responsibility for administering the code should also maintain a public list of companies who have satisfactorily completed self assessment.
4	This section is too broad and will need careful specification. It is also likely to lead to confusion about what is "in" and what is "out". The more options there are the greater the potential for obfuscation. ...self assessment is fundamentally flawed when attempting to protect the vulnerable against careless, incompetent or unscrupulous providers. ..The "additional modules" option is understandable but will result in a menu of compliance which may lead to more confusion and perhaps elitism. A simple and comprehensive set of compliance requirements without multiple options will server an under-informed market far more successfully

5	No Response
6	No Response
7	No Response
8	No Response
9	I think it is quite important to stick to the voluntary self-assessment code at this stage, notwithstanding some enthusiasm for random or compulsory audit referred to at 5.4. It is best to think about the code as a standard which will evolve over time. The first and most difficult stage is establishing a broad consensus about the text of the relevant provisions. If we don't get board industry buy-in from the outset, it is likely to die a quick death. Once that has been achieved, it can always be strengthened over time by adding more onerous obligations such as audit or a complaints procedure if necessary. Another compliance step which would be useful for individuals and is unlikely to cause significant difficulty for providers would be to require them to provide a contact point within their organisation where users can make complaints. In particular, for users to complain about any breaches of the code. This is also likely to be simplest and easiest to implement complaints resolution procedure to adopt at present. The costs of compliance will be minimal, and once the code is more embedded further down the line it could be expanded if need be. A more technical drafting point is that it might be best to cast the disclosure language (i.e. bullet point 3) in terms of "making available" the required disclosures, rather than "providing" these. If each provider has a detailed page on their website setting out these kinds of things so that anyone who is interested can view them that ought to be sufficient. Requiring each provider to send a standard form email (or attached PDF) with a lot of fine print each time they open an account may actually be counter-productive. A simple link to where the information can be found will probably do the job a lot better.
10	Sort of agree. Disclosure should be the first step. Without some form of audit process the code will lack credibility. At lease a sample of service providers must be audited to ensure they comply. It must be possible to legally enforce the withdrawal of a server provider's right to use the compliance logo/statement. This means that a fee must be charged of service providers for the right to say they comply with the code
11	No Response

12	I agree with the approach of an initial disclosure based code with a modular option available to suppliers, but on the understanding that there will eventually be a multi-tiered approach as the industry and code matures. I believe that a disclosures based code of practice is suitable for the nz industry.....and will gain a lot more participation this way. Self assessed code is fine initially but at some point there needs to be a more formal assessment eg, random audit to keep the applications honest and to ensure consistency in how the code is interpreted.
13	SUBMISSION REMOVED
14	[name removed] recommends that. A Key principle of any compliance or assessment measure is to ensure that the obligations do not move compliance with the code realistically beyond the majority of New Zealand businesses that the code is intended to apply to A review that is undertaken annual of the code to ensure ongoing relevance to the wider stakeholder needs
15	[name removed] recommends an annual review of the code, and that the following metrics be considered in such a review: Number of companies using the code Awareness amongst users of cloud services Satisfaction of suppliers and customers with the code Number of submissions to enhance the code. [name removed] also recommends that one focus of the upcoming workshops is to seek the definition of a complaints process
16	No Response
17	We think the disclosure based approach is a good one in the current environment. It puts the key information in the hands of the purchaser to assist their decision making. It also neatly complements our own approach to guidance. We found the use of "compliance" a little confusing. Although the overarching approach is disclosure-based, section 4.2 also includes standards-based elements, namely minimum security requirements, adherence to good practice guidelines, maintaining a professional service to clients, not engaging in conduct that is misleading or deceptive, meeting the formal definition of cloud computing. Assessing compliance with disclosure (has x disclosed all the items they are required to?) is quite different to assessing compliance with standards (does x adhere to good practice guidelines?) This mix of standards and disclosure elements will likely cause tensions when it comes to resolving the question of assessment in 5.4.

4. Areas of Disclosure

Based on the survey responses we have 10 areas of disclosure in the draft document. These areas are the standard set of disclosures that you must make to be code compliant.

Are there any areas that you do not agree should be included in the code?

Do you have further suggestions of areas of disclosure that must be made as part of the standard set of disclosures??

Responses

Respondent #	Submission
1	Below are our comments on the 10 stated disclosure points: Corporate Identity – The following should not be required to be disclosed: Trading start date, fax details, major shareholders (as many companies are listed companies) CEO Name. Many of these details add nothing and some of these will need to be updated from time to time and add more admin to this process. Ownership of Data – We agree with this disclosure Security - We agree with this disclosure. We recommend SAS70 and ISO 27001:2005 as the applicable compliance standards. There should be a range of standards as well as a core set of core standards Data Location - We agree with this disclosure Data Access - We agree with this disclosure Back up and Maintenance - We agree with this disclosure Geographic Diversity – We do not agree with the words “as determined independently”. This would cause providers to incur additional costs in seeking an independent opinion. An explanation of the geographic locations and the elements of the service provided from those geographies is sufficient to inform customers who can them make their own independent decision, seek further information or obtain their own advise SLA and Support – This disclosure requirement should make it clear that the provider is not required to have a committed uptime % SLA. Many providers will not provide a % availability commitment and it will up to them whether they have one or not. The provider should only be required to state either (i) if they do not have an SLA that they do not offer a generally available SLA , or (ii) if they do offer an SLA they may choose to disclose it and if they do disclose it then they should also clearly set out any exceptions to the SLA, how it is calculated and what remedies the customer has if the SLA is not met. Competency Warranty – this should not be in the code, it is a legal statement, not a disclosure. This is a matter to be dealt with under contract law or trade practices law compliance Privacy Policy - We agree with this disclosure

2	Some disclosures are appropriate in the areas of corporate identity, data ownership, security, data location, data access, back up procedures, SLA's and support, and competency. We do not agree that the information on the maintenance program should be a requirement of the code. It is unclear what the geographic diversity section is intended to cover and therefore whether this section is appropriate [name removed] is not commenting on the detail of each section at this time, however for the avoidance of doubt even where we agree that the heading areas are correct, we do not necessarily agree with the detailed descriptions and look forward to the appropriate consultation on these areas
3	The areas of disclosures for the code give disproportionate weight to the location of data and services, seemingly presenting them to potential cloud users as a significant risk factor. The 'Data location' disclosure element requires vendors to state the country or jurisdiction in which data will be permanently stored, mirrored or backed up: including highlighting the risks of storing data off shore. The 'geographic diversity' disclosure statement requires vendors to state the counties services are provided from and any risks. It is reasonable to give users some information about the location of data and services, including whether it will be stored onshore or offshore, but it should not be over emphasised as a risk factor. The location of data and services are no fundamental determinants of acquiring a cloud computing solution, rather, they are questions about how a particular provider implements the solution. The nature of global vendors with multiple datcentres (to ensure resilience of data and services) means that data may move between centres. It is not practical to have to constantly update which centres data will be stored in. Data is often stored in the network – not permanently in particular data centers........ Recommendation: the disclosures required by the code should only address whether data will be stored onshore or offshore. It should not require specific details of data and service locations to be disclosed, or statements of the risks involved, as this may encourage overly risk averse assessments
4	Security – there needs to be a uniform set of standards, otherwise less scrupulous providers may pick and choose. The CSA Standards should be the defacto standard unless the provider discloses why another option is more appropriate Data Access – there needs to be a more refined definition and explanation of the whole data lifecycle from initial engagement to completion of engagement.

5	In the Cloud Code Structure, an additional statement area that may be considered could be Payment for Services ie a description of exactly how the consumer will pay in a flexible, scalable and transparent manner. This could be complicated depending on exactly what is being procured, (data backup, server power, software licensing etc) however to fit with the measured pay-per-use philosophy it should be a Code preformatted statement. This section could include, measurement of $, (eg $500) usage (eg, per user), and timescale (per month), potentially set-up costs, and also state any minimum contract term, and minimum price (if any ie the minimum people would pay per month even if they did not use the service whatsoever). It may be beneficial to move away from getting providers to specifically state their back up procedures etc (which may be competitive advantage) and more towards a statement of uptime as a percentage or minutes per month/ year expected downtime. This will mean more to the general consumer and will enable easier comparison.
6	No Response
7	The structure refers to provision of disclosure to customers but, if cloud on-sellers are also to be bound then they also will need information from upstream cloud providers so that they in turn can provide it to customers – this may need to be dealt with separately
8	No Response

9	Structure (5) – location issues In practice, the “Geographic Diversity” disclosure (and “Jurisdictions” additional disclosure) are likely to give rise to a few difficulties. We need to be wary of all the complexities involved in the application of various laws to cloud enterprises in how we cast these required disclosures. The location of the data is certainly relevant, and disclosure of this is important. The dirt on which the servers sit is always going to be hugely relevant in terms of the applicable law. But of course, that isn’t the end of the story. Even if a multi-national service provider such as IBM stores the data entirely in NZ, it can still be required by a US court to disclose it to US authorities. People often talk about the Patriot Act, but actually the far more common scenarios are where the US parent is involved in litigation (and a court orders disclosure of information from a foreign subsidiary) or is subject to investigation by a US regulator (e.g. FTC) who demands such data. Likewise other jurisdictions are always likely to try and apply their laws if their citizens are involved, regardless of where the data is stored, or the company is based. The French government and courts, for example, are notorious for this in any circumstances where a French citizen’s information is at play. This stuff is quite difficult to get to grips with using an army of lawyers in the context of a specific fact scenario - thinking about all possible options in advance and dealing with them in a disclosure statement would be near impossible. I think it’s unlikely the average NZ service provider will be able to carry that out in a way that provides meaningful information for users. The consequences of where services are supplied from won’t always be apparent and also won’t necessarily be determinative of the jurisdictional question. Other factors, like the identity of the service provider company (e.g. Rackspace, Amazon) actually storing the data may well be more relevant. I recommend removing both these categories altogether. Downstream service providers On the other hand, parts from additional module 5.2, “Service Dependencies”, may actually be more relevant information for users to obtain from a privacy and jurisdictional point of view than some of the more general location information referred to above. It could also be disclosed without huge burdens by suppliers. I suggest moving a more limited version of this into the standard areas of disclosure. That is, each cloud provider could state as a minimum the names of service providers who will store data on behalf of the provider. Some of the other elements such as what will happen if that service provider goes out of business etc, could remain as additional modules.

	This is particularly relevant because in practice for many NZ SaaS providers, most of the substantive technical security measures will be undertaken by that downstream security provider (e.g. Rackspace, Amazon). That's why they are using them in the first place. Presumably, in order to comply with the security measures standard disclosure, these SaaS providers will just cut and paste the technical detail from their downstream service provider This actually gives rise to another point, which is whether a cloud code company which does outsource its data storage to an offshore or multinational supplier should be required to put in place certain contractual safeguards to protect such data. In reality the protection of the data by that service provider is only as good as the contractual terms in place, and often in the cloud context service providers will disclaim all responsibility contractually, even to maintain the confidentiality of data stored. A requirement to put in place contractual clauses has the potential to be quite onerous, but I'm sure we could probably come up with a form of wording that some of our multinational stakeholders supporting the NZ cloud code (e.g. Google, Microsoft) could be happy with. Perhaps it is a more appropriate idea for an "additional module". **Back up and maintenance** I also wondered if it was practical to include "Back up and maintenance" in the standard disclosures. Providers' practices re back-ups and maintenance are likely to change quite regularly, and if this is part of the standard disclosure it may be quite onerous and/or bureaucratic to have to amend those. Perhaps the pre-formatted statement could be kept very limited, with the technical detail contained on a separate link, which the organisation can update from time to time.
10	Please add data transportability and migration. A user of a Cloud service should have the right to access and extract their data at all times, even if the service provider has been placed into receivership. Also add dependence on upstream providers, disclosure of relevant jurisdiction and business continuity; i consider these to be mandatory disclosures

11	I would like to request that the definition of Geographic Diversity be expanded from its current state: "A Statement disclosing the countries in which services are provided from and the consequence of the service being provided from that location (if any) as determined independently" To include: Cities as well as countries Rationale: NZ companies currently have significant risk associated with poor geographic diversity of datacentre resources nationally. Especially notable is the vast concentration of datacentre resources in Auckland. The risks are many, and include things such as: geological disasters (earthquake, volcanic), hydrological disasters, meteorological disasters, health disasters, disasters affecting data and electricity supply, terrorist disasters, disasters affecting civil infrastructure (water, waste, transport). The code of practice should encourage distribution of cloud computing backend infrastructure across geographically diverse locations, and when data sovereignty is considered, this means across multiple cities within New Zealand. At a minimum, the disclosure requirements should call for a cloud computing provider to either: 1) Disclose the cities where their data centres are located, OR 2) Provide an assurance that the data centres are a minimum of xx kilometers apart (150km would be a reasonable minimum) The definition and disclosure around Data Location should also be expanded to include: 1) Cities as well as countries, OR an assurance about minimum geographical distance separation between each of 2), 3) & 4) below 2) Primary data location(s) 3) Secondary data location(s) (such as automatic failover sites) 4) Backup data location(s) (backup tapes, offline data vaults etc)
12	I Agree in general with the 10 areas of disclosure as per the Draft Document. A number of issues with these that i believe may need to be worked through are: Security – verifying compliance with a set of standards may be an issue......Would organisations feel that disclosing specified data security measures be giving away commercially sensitive information? Data Access – "disclosure of any proprietary elements to the way data is stored" would require organisations to release potentially commercially sensitive information.
13	SUBMISSION REMOVED

14	[name removed] recommends that the following disclosures are investigated: Software Licenses used and implications of those licenses on the transferability of a users systems. Software Escrow arrangements that are in place are listed
15	[name removed] seeks to ensure that inclusion of the following mandatory disclosures: Software Licenses used and implications of those licenses on the transferability of a users systems. Software Escrow arrangements that are in place are listed An assertion from services providers if the service is subject to foreign laws including a foreign governments lawful access to data held by the service provider
16	No Response
17	It is important to be aware that "ownership of data" is a concept that will only apply in a limited range of circumstances. We see it being particularly relevant in the event of a business going into receivership or similar circumstances, where the data may be seen as an asset by creditors. It is less relevant in the privacy context, where use of personal information is determined primarily by privacy law and contractual arrangements, not by ownership. There may also be other legal powers that affect ongoing access to data (for instance recent deletion of user data on megaupload). Does the "access" section only address client-side access? If not would provider-side access be addressed under "Maintenance and backup"? Not all provider-side access would seem to be addressed by this heading. For instance where data is encrypted at rest, the provider might still hold a key, but not necessarily for maintenance or backup purposes. Whether a provider can access data, and for what purposes they do access it for should be important considerations for a purchaser. "Geographic diversity" looks like it could be rolled in to "Data location". "Jurisdictions" also looks like it should fit under the same heading, although the aim may be to provide information on the jurisdiction, rather than just providing information on which jurisdiction the information is located in.

5. Additional Modules

There are 7 additional modules of disclosure set in the draft document. It is suggested that by subscribing to some or all of these modules organisations who are code compliant will be able to promote themselves as being a higher than standard level of compliance. For example someone who subscribes to 3 of these modules may be level 2, 5 modules could be considered level 3 and all 7 modules could be level 4.

Do you agree this is the best way to move forward with this type of model, or can you suggest a more effective model for recognising and rewarding organisations who elect to make these additional disclosures?

Responses

Respondent #	Submission
1	We agree with the proposed approach. We caution that these areas are highly technical and will vary greatly from provider to provider. It will be difficult to assess whether a disclosure is accurate and therefore if the provider has made a legitimate disclosure under the Code and is entitled to claim the higher level of compliance.
2	Although the majority of the additional modules appear to be appropriate, care is needed to ensure that the additional modules are actually relevant to the products and services being offered, so that organisations are not encouraged to comply with additional modules purely for the sake of achieving a higher "Tier" with no added customer benefit. It is unclear how "jurisdictions" differs from the location based disclosures in the main sections.
3	There is logic in the Code requiring a set of core disclosures that are fundamental for all providers complying with the Code, with the option for vendors to provide additional information on the core disclosures if they choose. For example, 'Security' practices being a core disclosure with 'Enhanced Security' on incident management being an additional disclosure. However, creating multiple tiers of compliance with different levels of disclosure may create unnecessary complexity and begin to move away from an industry code towards regulation. Such complexity could impose an unreasonable burden on small cloud providers and possibly hold back innovation in the sector. Recommendation: the levels of compliance should provide for a core set of disclosures, with an optional set of additional disclosures building upon the core ones.
4	As noted above in an earlier response, this will likely lead to more confusion. Multiple options and multiple tiers are a recipe for misunderstanding. The additional modules listed on page 11 are all meritorious and should be included in the base code. What user of cloud services would not want to know the provider's position in each of these modules? Why they are not included in the base code of conduct? Is there an objective of having some form of complaints authority or ombudsman process relating to the code?
5	There may be benefit in moving towards more industry focussed Modules – ie Government, or Finance, or Health, as these industries have specific rules which an organisation would need to understand before providing cloud services. I would not prescribe the suggested levels of cloud computing, ie lv3 or lv4, I do not think consumers will understand this. Perhaps something like, Compliant (is just the basic data), Expert (basic plus some additional) & Recommended (all additional disclosures). At the most I think 3 tiers would be understandable to the general users.

6	No Response
7	No Response
8	No Response
9	No Response
10	If my suggestions are adopted there will only be three additional modules. I don't think it will be useful to different the number of additional modules by the use of levels.
11	No Response
12	I do not agree with the suggestion of a tiered level of compliance - I believe it will be too hard to adequately ensure it was being used consistently. Rather have mandatory areas of disclosure as per 4 above and additional modules to which organisations may choose to subscribe. It also appears that much of the data requested in the additional modules would be confidential or proprietary information (eg details of proprietary data formats) which organisations will not wish to reveal.
13	SUBMISSION REMOVED
14	No Response
15	No Response
16	No Response
17	We consider that breach should be a core module. The Law Commission's recent review of the Privacy Act recommends compulsory breach notifications (albeit with a trigger or threshold) which means that this will become a legal requirement for many New Zealand businesses.

6. Other matters

Are there areas of disclosure here that you feel are missing or are superfluous?

Responses

Respondent #	Submission
1	No Response
2	Overall, the structure and approach taken gives [name removed] cause for concern that the code will lead to unnecessary differentiation between local and global providers, and in particular may discriminate against global providers and those who re-sell or consult on the use of their products. This could lead to NZ based businesses being unable or unwilling to access highly efficient, large scale products and services available to the rest of the world.
3	No Response

4	1. Plain English There is a strong international movement for the use of plain English language in insurance contracts, consumer-type legal agreements, as well as corporate legal agreements. There is an international body which promotes this. While the challenge of communication with IT technical language is daunting, this is even more reason that plain English should be used in all public-facing disclosures of compliance. Definitions, explanations and careful wording should be an imperative. A reader of the disclosures should not need to be a technical IT person to understand the disclosures and the implications for their business or themselves. 2. What Does It Mean and Why Should I Care? This follows from the plain English note above. Readers of a provider's compliance statement should be able to understand the relevance and consequences of different disclosures. The code should promote more than just a disclosure statement; it should also provide a form of education so that users may become better informed. The better informed a potential user is, the more likely they will make a good decision. 3. What Happens If My Cloud Provider Goes Out of Business? This should be more than a DR plan. What happens to my data if my provider fails commercially? This is a recurring thought in anyone's mind as precious data is handed to a third party. While upstream providers are considered in the "optional modules" section, this is not sufficient protection for the user organisation. The primary provider must be considered. This is a key problem that should be addressed by legislation and not just by a voluntary code of compliance. 4. Roadmap to Legislative Protection There must be an active roadmap process to enshrine elements of the code into a regulatory framework in the near future. The full data life-cycle is the most critical element required to be under legislative control. Most other elements of the code are in the nature of marketing differentiators. A voluntary self-assessment of compliance is toothless and will not provide protection for the more vulnerable users of cloud computing services.
5	No Response
6	See supplementary submission "RNZFB submission"

7	An initial very high level summary of the code and what consumers might expect a signatory to provide (with links to the main disclosure section in particular). It is important that the code is accessible to non-technical consumers for some of whom, tldr may prevent them reading more than the first page ;-) a definitions/glossary section. No doubt there will be terms other than “cloud” which will need to be clarified. A robust complaints procedure (note that this may need to involve both a cloud provider and an on seller if they are both involved in providing service to an end customer but should not be able to be used for disputes between providers and on sellers) legal status of code – is it a contract between provider and customer? Must provider incorporate it by reference into its Ts & Cs? I’d like to see use of explanatory examples in the code as sidebars to the main text.
8	No Response
9	No Response
10	No Response
11	No Response
12	No Response
13	SUBMISSION REMOVED
14	No Response
15	No Response
16	No Response
17	No Response

Additional notes:

Respondent # 6 provided numerous grammatical and spelling corrections in their submission, all of which have been included in the final document.

Respondent # 13 has provided lengthy discussion on the background to their recommendations which have not been included in this document but will be discussed in the Final structure discussion document.