

# The Cloud Industry Forum Cloud Service Provider Code of Practice:

Conducting the Self-Certification

# 2



[www.cloudindustryforum.org](http://www.cloudindustryforum.org)

# Table of Contents



SUPPORTED BY



<b>Purpose of this Document</b>	3
Process Stages Covered Within this Document	3
<b>Conducting the Self Certification</b>	4
Prepare	4
Assess	4
CIF Code of Practice Requirements and Guidance	5
<i>The Cloud Industry Forum (CIF) Code of Practice (v6.1)</i>	5
<i>Section A. Transparency</i>	6
<i>Section B. Capability</i>	9
<i>Section C. Accountability</i>	11
<i>Other Information Required for Application</i>	12
Improve	13
Declare	13
Validate	14
Authorize	14
Publish	14
Next Steps	14
<b>Further information</b>	14
Governance of The Code Of Practice	14
About the Cloud Industry Forum (CIF)	14
The CIF and The APM Group Limited (APMG)	15
Code Governance Board	15
Development and Maintenance of the Code	15
Audit and Appeal	16
Collaboration with Standards organizations and related Bodies	16
Contact Us	16

The CLOUD INDUSTRY FORUM and CIF words and associated logos are trade marks. © Cloud Forum IP Limited 2013. All rights reserved

NOTICE: This document is intended to provide general information in relation to the Cloud Industry Forum's Code of Practice journey for Certification. It is not intended to be comprehensive and should not be acted or relied upon as being so. Professional advice appropriate to specific circumstances should always be obtained.

## Purpose of this Document

This document (Document 2) is aimed at organizations that have registered, or are considering registration for the Cloud Industry Forum (CIF) Cloud Service Provider (CSP) Code of Practice (Code) Self-Certification.

This document incorporates guidance to support the specific Self-Certification requirements from the “Code of Practice” supported by further information on the Preparation, Assessment, Application (Declaration) and Post-Application stages of the process.

Organizations should also download and refer to the following information provided by the CIF, downloadable from the CIF website [www.cloudindustryforum.org](http://www.cloudindustryforum.org):

- Document 1: An Executive Briefing
- Document 3: Guidance for Cloud Service Providers
- Terms and Conditions for Self-Certification
- Cloud Service Provider Code of Practice

Further information or guidance can also be sought directly from the CIF ([info@cloudindustryforum.org](mailto:info@cloudindustryforum.org)) or APM Group, CIF's Independent Certification Partner ([servicedesk@apmgroupltd.com](mailto:servicedesk@apmgroupltd.com)).

## Process Stages Covered Within this Document

This document covers the following stages of the Self-Certification process:

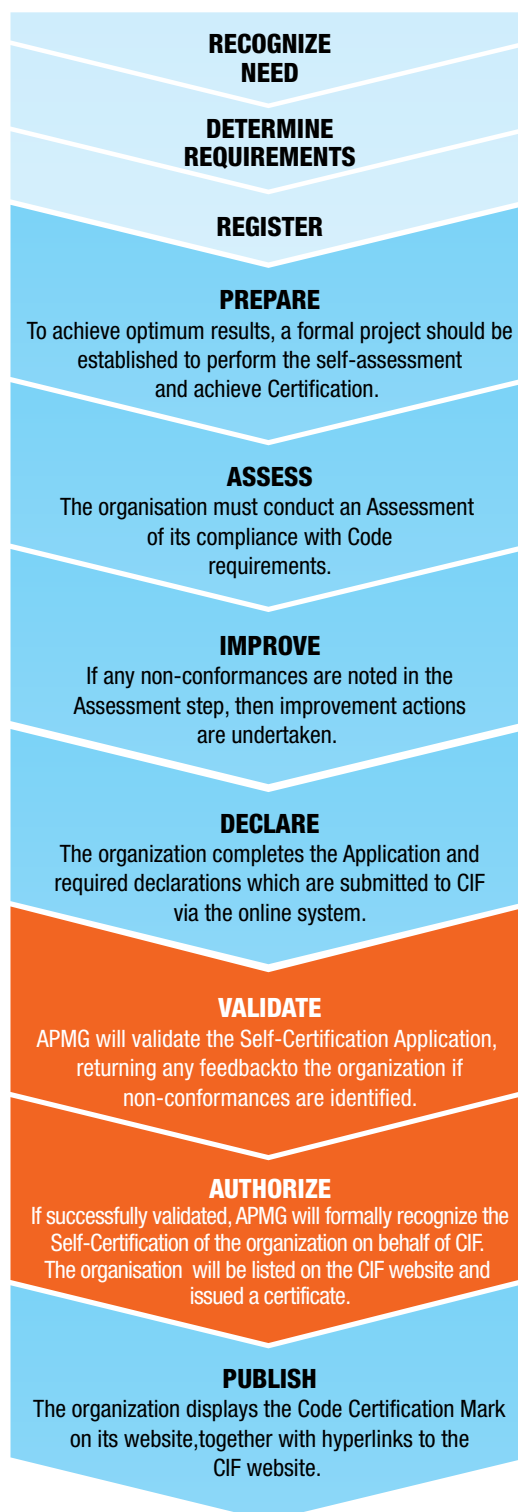
- Prepare
- Assess
- Improve
- Declare
- Validate – APMG Activity
- Authorize – APMG Activity
- Publish

For information on the Business Case and details of how to Register for Self-Certification, refer to the following document:

- Document 1: An Executive Briefing

For additional information and instructional guidance, see also:

- Document 3: Guidance for Cloud Service Providers
- Cloud Service Provider Code of Practice
- Terms and conditions



## Conducting the Self Certification

Once a CSP has made a commitment to the process, the next stage is the detailed activity involved in Self-Certification and making the formal application for validation to the CIF. The CSP must be comfortable that it is appropriately prepared for the activities involved in these stages to avoid missing the timeline for certification, or the late realization that the organization cannot meet the requirements in full.

### Prepare

To achieve optimum results, a formal project should be established to perform the self-assessment and achieve Certification. At a minimum it should include creation of a project charter, team and plan, and an electronic filing system for supporting documentation. Existing information relating to transparency and capability should be gathered. If any of these do not yet exist, they should be created at this point in order to apply.

In addition to the guidance provided within the “Ensuring adequate Preparation section’ of Document 1: An Executive Briefing”, the minimum steps identified by the CIF required for adequate preparation after registration are:

#### Identify the Self-Certification Team Leader or Project Manager.

This person will oversee the entire Self-Certification process for the CSP. This individual should have the required time to dedicate to the project, as well as the authority, experience and skill - or access to the necessary internal resources with these qualities - to gather all evidence of compliance required for Application.

**Download, read and ensure understanding of ALL documentation.** It is critical that the Team Leader or Project Manager overseeing the process conducts this step. They must have an understanding of what is required at each stage of the process and what each Code requirement is “asking for”, but they should also be able to identify and locate specific documentation that may need to be passed on to other project team members for them to fulfill their assigned tasks. In addition, some documentation provides guidance only whereas others include prescriptive, mandatory instructions, which must be followed to meet particular requirements.

**Establish a system for organizing supporting documentation.** The CIF provide clear guidance on the format and naming conventions that must be used when submitting supporting documentation within “Document 3: Guidance for Cloud Service Providers”; however, organizations should also ensure they have an appropriate system for managing documentation (including version control) during the Assess and Improve stages prior to submitting the Application.

**Review preparation plans and clarify what additional help/guidance may be required or available.** This support can be sought from the CIF via the [AdminSC@cloudindustryforum.org](mailto:AdminSC@cloudindustryforum.org) address.

A Preparation Checklist is included in both “Document 3: Guidance for Cloud Service Providers”, and in the Assessment Spreadsheet, to aid in preparation activities.

## Questions to answer before moving to the next step of the Self-Certification process

- **have you downloaded and reviewed all documentation in full, including additional documents such as templates and guidance documentation?**
- **have you prepared appropriately considering:-**
  - **The 6-month timeline for completion of the process,**
  - **The input and resources you have within the project team (if any), and**
  - **The technical requirements of the Code and the process for Self-Certification**

### Assess

The Assessment stage is the detailed self-assessment of internal processes and documentation, together with external public-facing information sources to ensure compliance with the requirements of the Code of Practice.

At this stage, CSPs should also refer to “Document 3: Guidance for Cloud Service Providers”, which includes templates and guidance documents relevant to the presentation of information and documentation for validation by APMG. CSPs should use the Assessment Spreadsheet Template provided by the CIF to cross-reference Code requirements to existing information sources. This will identify any gaps or areas that need improvement or attention. The form can also be used to record specific document references e.g. filenames and clauses for entry into the online system later at application.

At this stage, CSPs should ensure that required public disclosure information will be available on the organization’s website (see section A.1 of the Code of Practice) in the required format before the application is submitted, and that contracting disclosure information is similarly available or developed.

If there are any questions about whether a requirement is met, or if it is not relevant (under the ‘comply or explain’ principle), the CIF or APMG can be contacted to provide guidance or issue a numbered Exemption if appropriate. Exemptions are issued as a alphanumeric code which can be entered into the online system upon application and all Exemption requests are processed by sending the request in writing to [AdminSC@cloudindustryforum.org](mailto:AdminSC@cloudindustryforum.org) for review by the Code administrators, APMG. All Exemption requests will be considered on a case-by-case basis and on their own merit.



# CIF Code of Practice Requirements and Guidance

This section identifies and provides guidance in relation to the Self-Certification requirements which organizations are required to comply with as defined by the Code of Practice (Code), and details of additionally stipulated requirements including the Professional Reference and Management Declaration.

Applicants are required to provide evidence of compliance with these requirements via a variety of methods. Specific guidance on the presentation and submission of evidence to the CIF for validation of the Self-Certification can be found in the accompanying “Document 3: Guidance for Cloud Service Providers”, which should be referenced alongside this document.

## NOTE:

The Code of Practice Requirements outlined herein do not represent the definitive Code of Practice in its entirety. Instead, this section includes extracts from the full Code of Practice (v6.1) incorporated with guidance to support applicants through the Self-Certification process.

Applicants must therefore download and refer to the stand-alone Code of Practice (downloadable from [www.cloudindustryforum.org](http://www.cloudindustryforum.org)) when conducting the Self-Assessment.

To differentiate between Code extracts and supporting guidance, all requirements taken directly from the Code are identified in italics.

## Code of Practice for Cloud Service Providers

*This Code of Practice for Cloud Service Providers (“Code”) from the Cloud Industry Forum (“CIF”) is for organizations offering to customers remotely hosted IT services of any type. These services include, but are not limited to, multi-tenanted services accessed via the Internet.*

For clarification, the Code is most suitable for organizations who fulfill the following requirements:-

- Provide access to IT services (i.e. Cloud application(s) or Infrastructure as a Service) and
- Have a direct contract for supply of these services with the purchaser (i.e. reseller, corporate or individual).

*Organizations claiming compliance with the Code shall conduct an annual Self-Certification and confirm the successful results of this Certification to the CIF in order to receive authorization to use the Certification Mark (the ‘logo’) for the following year.*

*The Self-Certification claims will be listed on the CIF website (<https://selfcert.cloudindustryforum.org/certification>) and hyperlinked from the logo displayed on the participant site.*

*The CIF may spot check and randomly audit Self-Certifications and will investigate any formal complaint of non-compliance against an organization claiming compliance with the Code.*

*In the event of finding a false declaration or material non-conformity, at the sole discretion of the CIF, the authorization to use the Certification Mark shall be immediately suspended, pending resolution, or terminated, and this action shall be documented on the CIF website, and may be reported publicly such as via press releases.*

## SECTION A. Transparency

***The first and most important pillar of the Code is to ensure a reasonable and consistent level of transparency about businesses and their operational practices throughout the Cloud Industry.***

***The Code does not specify best practice in Cloud Computing except with respect to transparency.***

*Organizations complying with the Code shall conduct themselves in an open and transparent manner that facilitates rational decision-making and management by purchasers of their services. The Code, however, does not set out to and will not make decisions for purchasers, but will simply help to ensure that essential information is available to make decisions.*

*There are two categories of information, which shall be disclosed:*

- A.1. Information for public disclosure; and
- A.2. Information for contracting disclosure, which may either be publicly disclosed or commercial-in-confidence subject to non-disclosure terms.

### A.1. Information for Public Disclosure

*Information for public disclosure should be readily available on the organization’s website in the format and location specified by the CIF, with a hyperlink to the CIF website: <https://selfcert.cloudindustryforum.org/certification> (see Document 3: Guidance for Cloud Service Providers for specific instructions on presentation of information). The CIF website will also have available the relevant information which was provided at the time of the certification application.*

*The information on the organization’s website should be kept up-to-date (within 4 weeks of changes occurring), whereas the CIF website will be updated only as part of the annual certification application process.*

*Optional categories of information (designated below by ‘Optional’), if publically disclosed, shall include all of the types of information shown for each category. Any optional categories of information that are not publically disclosed shall be disclosed as part of “Information for Contracting”. (Disclosure of Industry Association Memberships is optional in both cases).*

To meet the requirements of this section, an applicant organization is expected to:

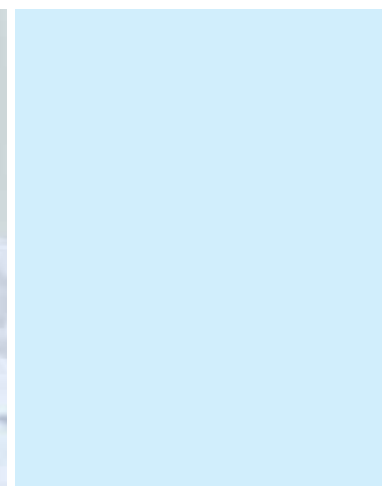
- Have a live, public webpage accessible from the home page of their website and linked to the CIF website, including all applicable information within this section; and
- Enter all of the information required against this section of the Code into the online application system.

See the following table for information and further details on how to provide evidence of compliance against each of the Code requirements within section A.1.

	Code of Practice Requirement	Evidence of Compliance
<b>A.1.1 Compliance with the Code</b>	<p>Statement that the organization commits to complying with the Code for the scope covered by the Application (defined in A.1.3).</p> <p>Link to the organization's website page where publicly disclosed information is available, including statement of commitment to complying with the Code.</p>	<p>Post-Registration Statement to be reproduced on the organization's website(s)</p> <p>Information to be entered into online system</p>
<b>A.1.2 Corporate Identity and Responsibilities</b>	<p>[Note: The information in this section is required for the legal entity which contracts with the purchaser of cloud services covered by the Code. It should not be a separate marketing or operational entity.]</p> <ul style="list-style-type: none"> <li>• Corporate name</li> <li>• Legal status, date of formation, location of registration, and registration number</li> <li>• Ownership (major shareholders)</li> <li>• Members of board of directors (or equivalent body)</li> <li>• Executive management (CEO and CFO or equivalents)</li> <li>• Corporate fixed address [not a post office (PO box)]</li> </ul>	<p>Information to appear on the organization's website(s)</p> <p>Information to be entered into online system</p>
<b>A.1.3 Scope Covered by the Code</b>	<p>Note: The online system facilitates provision of this information via both free-text for definitive statement of scope (which will typically include product or service names) and multiple selection drop-downs (for services and geographies) to facilitate customer searches.</p> <ul style="list-style-type: none"> <li>• Scope of services</li> <li>• Geographical scope</li> <li>• Countries with local sales and/or support</li> <li>• Countries where customer data may be held or processed</li> <li>• Statement about whether the customer can restrict the countries where customer data may be held or processed</li> </ul>	<p>Information to appear on the organization's website(s)</p> <p>To be entered into the online system via free text and drop down selection</p>
<b>A.1.4 Public Branding</b>	<p>[Note: The information in this section is only for the scope of services covered by the Code].</p> <ul style="list-style-type: none"> <li>• Alternative trading name(s) if different [Any alternative marketing or trading ("doing business as") names]</li> <li>• Website address(es) [Websites used to market the services covered by the Code (whether owned by the contracting legal entity or not). All of these websites must provide the information for public disclosure required by the Code.]</li> </ul>	<p>Information to appear on the organization's website(s)</p> <p>Information to be entered into online system</p>
<b>A.1.5 Third Party Coverage Transparency</b>	<p>Statement about the extent to which the organization accepts indirect responsibility for the organization's suppliers.</p>	<p>Information to appear on the organization's website(s)</p> <p>Information to be entered into online system</p>
	<p><i>This covers the situation of the organization's suppliers going out of business. For example for the technical failure of vendors in the supply chain such as collocation where services are taken off-line.</i></p>	
	<p>Statement about the extent to which the organization's suppliers accept indirect responsibility to the organization's customers.</p>	<p>Information to appear on the organization's website(s)</p> <p>Information to be entered into online system</p>
	<p><i>This covers the situation of the organization itself going out of business. For example if the organization aggregates third-party services that are on-sold to the organization's customers, do the third-party supplier contracts offer reciprocal terms and protections e.g. liability, service level resolution, data protection?</i></p>	
	<p>Statement about extent to which the organization accepts indirect responsibility to customers of customers</p>	<p>Information to appear on the organization's website(s)</p> <p>Information to be entered into online system</p>
	<p><i>This covers the situation of the organization's direct customers going out of business. For example, to customers of customers for access to data if the direct customer goes into administration or liquidation</i></p>	



	Code of Practice Requirement	Evidence of Compliance
<b>A.1.6 Security Control Transparency with the Cloud Security Alliance</b>	<i>Statement about whether the organization has completed the Consensus Assessments Initiative Questionnaire from the Cloud Security Alliance (<a href="https://cloudsecurityalliance.org/cai.html">https://cloudsecurityalliance.org/cai.html</a>), which "provides a set of questions which a cloud consumer and cloud auditor may wish to ask of a cloud provider" to provide "security control transparency".</i>	Information to appear on the organization's website(s)  Status to be confirmed via online system (Yes/No checkbox)
<b>A.1.7 Other Extended Commitments to Code of Practice Principles</b>	<i>Statement about whether the organization commits to any additional transparency, capability, or accountability requirements in addition to those contained directly in this Code of Practice.</i>	Information to appear on the organization's website(s)  Information to be entered into online system
<b>A.1.8 Technological Commitments</b>	Optional disclosure location (public or private): <i>Statement about whether there are any specific technologies, standards, or inter-operabilities which the organization commits to supporting.</i>  <i>There is no requirement to support any specific technologies etc, but it should be clearly stated whether there are any such commitments. Standards may be formal or under development, as long as they are specifically referenceable.</i>  <i>Reference to where relevant information about the technology, standard, or interoperability can be obtained.</i>	Information to appear on the organization's website(s) <b>OR</b>  Information to be submitted with documentation provided in support of section A.2.  Information to be entered into online system
<b>A.1.9 Existing Certifications</b>	Optional disclosure location (public or private): <ul style="list-style-type: none"> <li>• <i>List of any existing relevant certifications e.g. ISO 9001, ISO/IEC 27001, PCI DSS, SAS 70 and SSAE 16/ISAE 3402.</i></li> <li>• <i>Statement of scope of business covered by Certification, and how it corresponds to scope of Code.</i></li> <li>• <i>By whom certification was performed, if independently certified.</i></li> </ul>	Information to appear on the organization's website(s) <b>OR</b>  Information to be submitted with documentation provided in support of section A.2.  Information to be entered into online system
<b>A.1.10 Industry Association Membership (optional)</b>	Disclosure of this information is fully optional, however if they chose to disclose this information, the following should be confirmed. <ul style="list-style-type: none"> <li>• <i>List of any industry associations in which the organization has a membership.</i></li> <li>• <i>Reference to the organization's website.</i></li> </ul>	If disclosed:  Information to appear on the organization's website(s) <b>OR</b>  Information to be submitted with documentation provided in support of section A.2.  Information to be entered into online system



## A.2. Information for Contracting Disclosure

This information is for disclosure in connection with proposals and contracts.

Where contracts are individually negotiated and signed, this information will typically be subject to non-disclosure terms. When contracts are non-negotiable, and typically signed online, then this information shall be made available prior to contract signing.

This could be by means of disclosure on the organization's website, by hyperlinked reference in the organization's contractual terms and conditions, or in any other way.

To the extent that a customer will rely on any of this information, or on publicly disclosed information, it should be made part of contractual terms and conditions.

It is strongly recommended that an applicant organization prepare or provide a prototype document which includes all of the required information as specified in section A.2, which may become a base document to be modified as required for prospective customers.

Additional documentation may also be referred to and provided e.g. T&C's, price sheets, user guidance, processes and procedures etc.

An alternative to providing a prototype is to provide an actual example of what is or has been provided to a customer in a format that allows for easy mapping to the contracting disclosure requirements of the Code.

This information is treated confidentially and will only be reviewed by APM Group, the CIFs independent certification partner.

To meet the requirements of this section, an applicant organization is expected to:

- Submit documentation that includes the information required against this section of the Code, via the online system;
- Submit all documentation in electronically signed Adobe pdf format, ensuring all files have been saved according to the naming conventions stipulated by the CIF; and
- Confirm that each requirement area has been met via the online system, including details of the specific location of this information e.g. specific page numbers or document section references.

See Evidence of Compliance column below for further details.

See the following table for information and further details on how to provide evidence of compliance against each of the Code requirements within section A.2.

	Code of Practice Requirement	Evidence of Compliance
<b>A.2.1 Commercial Terms</b>	<i>Pricing policy (basis of charging with fully-declared costs)</i> <ul style="list-style-type: none"> <li>• Payment terms</li> <li>• Contract lengths and options for discount for longer commitment</li> <li>• Termination basis, terms and conditions</li> <li>• Renewal and amendment terms and process</li> </ul>	Prototype contracting disclosure document <b>OR</b>  Example agreement/contract <b>PLUS</b> Any additional supporting documentation (as required.)
<b>A.2.2 Personnel Profile</b>	<ul style="list-style-type: none"> <li>• Number of full-time personnel by band: (1-10, 11-50, 51-200, 201-1000, 1000+)</li> <li>• Number of staff based outside of the defined territory by band: (1-10, 11-50, 51-200, 201-1000, 1000+)</li> <li>• Employee vetting procedures undertaken</li> </ul>	Documentation to be electronically signed and uploaded to the online system
<b>A.2.3 Customer Migration Paths at Contract Termination</b>	<ul style="list-style-type: none"> <li>• Declaration of any commercial restrictions</li> <li>• Technological implications ( e.g. is there technological lock-in that prevents migration to other suppliers or in-house)</li> <li>• Format of data provision and transfer</li> <li>• Cost implications (e.g. are there any costs associated with recovering data, or for purchasing replacement licenses)</li> </ul>	
<b>A.2.4 Customer Migration Paths during Contract Execution</b>	<ul style="list-style-type: none"> <li>• Implications in the event of the organization itself, or the organization's suppliers, changing their provision of services, or ceasing business (e.g. is there technological lock-in with a specific supplier)</li> <li>• Ability to retrieve data in such situations</li> </ul>	
<b>A.2.5 Licensing Provision</b>	<ul style="list-style-type: none"> <li>• Who is responsible for any software/IP licensing, and any costs involved which are not covered within the cost of the services being provided?</li> <li>• Whether there are any licensing implications in addition to cost, including in particular whether *GPL is used potentially requiring publication of all code whether original code modified or not</li> </ul>	



	Code of Practice Requirement	Evidence of Compliance
<b>A.2.6 Provisions for Information Security</b>	<ul style="list-style-type: none"> <li>Overview of measures in place to provide for information security in general</li> </ul>	Prototype contracting disclosure document <b>OR</b> Example agreement/contract
<b>A.2.7 Data Protection Provisions</b>	<ul style="list-style-type: none"> <li>Countries and locations where data will/may be held during the term of the contract, and where processing will/may take place including for backup purposes</li> <li>Data protection legislation which will be relevant to the contract</li> <li>Overview of measures to ensure compliance with relevant legislation and to ensure data privacy</li> </ul>	<b>PLUS</b> any additional supporting documentation (as required).  Documentation to be electronically signed and uploaded to online system
<b>A.2.8 Provisions for Service Continuity</b>	<ul style="list-style-type: none"> <li>Overview of measures, including redundancy, to provide for service continuity including protection against data loss</li> </ul>	
<b>A.2.9 Provisions for Audit</b>	<ul style="list-style-type: none"> <li>Ability to arrange independent audits of the provider organization for various purposes e.g. security, license compliance and CIF audits</li> </ul>	
<b>A.2.10 Service Dependencies</b>	<ul style="list-style-type: none"> <li>Clarification of any sub-contracting or co-location relationships (names may or may not be given)</li> <li>Implications of service dependencies for service levels</li> <li>Compliance with data protection requirements</li> <li>Continuity of operations</li> </ul>	
<b>A.2.11 Complaints and Escalation Procedures</b>	<ul style="list-style-type: none"> <li>Complaint procedures</li> <li>Escalation procedures and named individuals for escalation</li> </ul>	

## SECTION B. Capability

***A second pillar of the Code is ‘capability’, by which is meant the ability of an organization to perform essential management functions, as demonstrated by having in place auditable documented management systems. ‘Capability’ is fundamentally different from ‘transparency’, although there should be a reasonable degree of transparency about capability. For this reason there are a number of requirements in the ‘transparency’ section about capabilities, but those disclosure requirements are not the same as actually having documented management systems in place.***

*Note that there is no disclosure requirement for the details of the management systems specified by this pillar of the Code. The CIF itself may audit these management systems, but the organization does not need to say anything publicly about these systems, except to the extent that they are covered by general disclosure requirements in Section A.*

Capability areas B.1 – B.4 are areas specifically covered by ITIL® Best Practices in service management, which can be referenced by organizations seeking general guidance. Areas B.5 - B.7 are not explicitly covered by ITIL at the same level, but are considered critical to success for organizations operating in the Cloud Industry. (ITIL® is a registered trade mark of the Cabinet Office.)

The extent of documented systems needed to meet the requirements of the Code will vary depending on organizational size and maturity; however a minimum level of documentation will be needed to meet all requirements.

It is expected that Information security management would typically require more extensive documentation, even in smaller organizations, and include for example a list of the regular information security control checks and reviews which are to be performed.

There are two ways of demonstrating capability at the time of application for Self-Certification:

- **Using Primary Documentation.** Providing primary management system documentation of required capabilities, including key policy and procedure-type documentation; or
- **Using Existing Certifications.** Providing evidence of appropriate existing certifications against relevant standards covering the same capability requirements (see Permitted Alternative Evidence column for details of the certifications accepted)

For more information see “Document 3: Guidance for Cloud Service Providers”.

*Organizations complying with the Code may wish to consider certification against relevant standards for the requirements of this section, such as ISO 9001:2000 or ISO/IEC 27001:2005. For smaller organizations that do not consider such certifications appropriate, the CIF may in the future develop prototype management system documentation for the required areas.*

To meet the requirements of this section, an applicant organization is expected to:

- Submit documentation that includes the information required against this section of the Code, via the online system;
- Submit all documentation in electronically signed Adobe pdf format, ensuring all files have been saved according to the naming conventions stipulated by the CIF; and
- Confirm that each requirement area has been met via the online system, including details of the specific location of this information e.g. specific page numbers or document section references.

During validation of the Self-Certification, documentation will be checked for its applicability to the capability area cited to ensure that it includes content expected of the documentation type (e.g. policy, procedure etc), but the check will not assess how “fit-for-purpose” the management system or documentation is. If a full audit is conducted, then this would be considered.



See the following table for information and further details on how to provide evidence of compliance against each of the Code requirements within section B.

	Code of Practice Requirement and Evidence of Compliance	Permitted Alternative Evidence
<b>B.1 Information Security Management (incl. Data Protection)</b>	<p><b>The specific areas for which documented management systems are required for the Code are:-</b></p> <p><b>1. Written Policies:</b></p> <p>These do not necessarily have to be extensive but should cover how/what the organization aims to achieve from a capability area. However the policies have to be sufficient to support the objectives of the company.</p> <p><b>2. Written Procedures:</b></p> <p>These may include work instructions, flow charts, service/operational level agreements; third party contracts; workflows built into management applications etc.</p> <p><b>3. Specific Individuals assigned with relevant responsibilities:</b></p> <p>These can be evidenced via organization charts, person specifications, job descriptions, RACI Responsibilities for these areas etc.</p> <p><b>4. Appropriate training and awareness programs:</b></p> <p>These may take the form of training plans or communications to others for awareness e.g. meeting minutes, internal memos etc.</p> <p>The CIF recognize that training may not always be required if resources are already fully competent however, it is expected that there is some provision to inform those employed or contracted where they can be impacted or can impact others. For example, if they do not appreciate the requirements for Data Protection.</p>	ISO/IEC 27001 certificate plus scoping statement CIF Code of Practice (CoP) self-certified partner certification plus scoping statement
<b>B.2 Service Continuity Management</b>		BS 25999 certificate plus scoping statement CIF CoP self-certified partner certification plus scoping statement
<b>B.3 Service Level Management</b>		ISO/IEC 20000-1 certificate plus scoping statement CIF CoP self-certified partner certification plus scoping statement
<b>B.4 Supplier Management</b>		ISO/IEC 20000-1 certificate plus scoping statement ISO 9001 certificate plus scoping statement CIF CoP self-certified partner certification plus scoping statement
<b>B.5 Software License Management (incl. License Compliance)</b>		ISO/IEC 19770-1 certificate plus scoping statement CIF CoP self-certified partner certification plus scoping statement
<b>B.6 Complaint Handling</b>		ISO 9001 certificate plus scoping statement CIF CoP self-certified partner certification plus scoping statement
<b>B.7 Environmental Impact Management</b>		ISO 14001 certificate plus scoping statement CIF CoP self-certified partner certification plus scoping statement

## SECTION C. Accountability

**Organizations that assert compliance with the Code shall be accountable for their compliance with the Code and for their behaviour with customers.**

### C.1 Accountability for Compliance with the Code

The CIF will revoke the Certification of any organization deemed not to be complying with the Code. Furthermore, this revocation will be publicized on the CIF website, and potentially be reported publically such as via press releases.

Potential non-compliance with the Code may be brought to the attention of the CIF in two separate ways:

a) as the result of customer or whistle-blower complaints to the CIF; and

b) as a result of spot check and random audits conducted by the CIF itself, or its appointed agents.

Customer or whistle-blower complaints may also result in such audits being conducted.

To enable auditing by the CIF of compliance with the Code, an organization shall maintain auditable records to demonstrate its compliance for a minimum of 14-months; extended during any period while an active the CIF investigation or audit has been notified to the organization.

The dated records to be maintained shall include:

- Copies of information for public disclosure as shown on the organization's website(s) and updated from time to time
- Copies of information for contracting disclosure, whether as shown on the organization's website(s) and updated from time to time, or as separately disclosed to potential customers, identifying those potential customers.

## C.2 Accountability for Behaviour with Customers

Organizations complying with the Code shall make two provisions to provide accountability for behaviour with customers:

- Provision of formal procedures for complaint resolution within the organization itself
- Willingness to agree to binding arbitration in local courts for the settlement of disputes. The CIF can provide expert witnesses to facilitate such arbitration.

These accountability requirements are separate from any which are created by legislation or regulation such as accountability

to adhere to the principles and guidance of the Advertising Standards Agency in the UK in regard to web-based content and advertising.

To meet the requirements of this section, an applicant organization is expected to:

- Confirm acceptance of both accountability areas via the online system; and
- Submit a Management Declaration (see Other Information Required for Application section of this document for further details on this requirement).

	Code of Practice Requirement	Evidence of Compliance
<b>C.1 Accountability for Compliance with the Code</b>	<p>Organizations which assert that they are complying with the Code shall be accountable for their compliance with the code and for their behavior with customers.</p> <p>CIF will revoke the certification of any organization deemed not to be complying with the Code. Furthermore, this revocation will be publicized on the CIF website, and potentially be reported publicly such as via press releases.</p> <p>Potential non-compliance with the Code may be brought to the attention of the CIF in two separate ways: (a) as the result of customer or whistle-blower complaints to CIF; and (b) as a result of spot check and random audits conducted by CIF itself, or its appointed agents.</p>	<p>There is no data entry required at this point. The organization demonstrates its compliance with this part of the Code by the online Management Declaration, which is made as part of the submission of the Application.</p>
<b>C.2 Accountability for Behaviour with Customers</b>	<p>Organizations complying with the Code shall make two provisions to provide accountability for behavior with customers:</p> <ul style="list-style-type: none"> <li>■ Provision of formal procedures for complaint resolution within the organization itself</li> <li>■ Willingness to agree to binding arbitration in local courts for the settlement of disputes. The CIF can provide expert witnesses to facilitate such arbitration.</li> </ul> <p>Complaint handling is covered by clause B.6 of the Code. The second requirement of this clause is covered by the following declaration:</p> <p>We are willing to agree to binding arbitration in local courts for the settlement of disputes.</p>	<p>Acceptance of statement /declaration via online system (checkbox)</p>

## Other Information Required for Application

### Management Declaration

**The purpose of the Management Declaration is to provide documented acceptance and commitment to the principles of the terms and conditions for certification and Code of Practice at a senior management level. It is made as part of the online Application process.**

When the online application is formally submitted, an email will be sent to a named senior executive (whose title and email address are entered into the online system) to confirm the Management Declaration which has been recorded in his/her name, and a confirming response is required to complete the application.

The content of the Management Declaration is predetermined by the CIF. See "Document 3: Guidance for Cloud Service Providers" or the Management Declaration Template for details of the content of the declaration. The content should not be altered by the organization.

As this process is partially automated, reliance is placed on the organization's internal procedures to ensure that the relevant member of management who will receive the email has been informed that their input and action is required, and that they have properly approved the Management Declaration.

The content of the Management Declaration will be available on the CIF website together with other publicly available information about the certified organization, showing the executive's name and position, but not the email.

To meet the requirements for the Management Declaration an applicant organization is expected to submit their Management Declaration unedited via the mechanism stipulated by the CIF. The email signature and address of the sender will be used together with the information submitted via the online system to cross-reference and validate all submitted Declaration emails.

## Professional Reference

**The purpose of the Professional Reference is to provide documented validation or authentication that the CSP is an established organization that has a professional relationship with another external third party organization or individual with professional standing within industry.**

The signed Professional Reference should come from the organization's registered accountant, solicitor, certification body auditor, or similar organization that provides professional services to the CSP on an on-going basis. See "Document 3: Guidance for Cloud Service Providers or the "Professional Reference Template" for details of the prescriptive content of the declaration. The content should not be altered by the organization or their referee and should be reproduced exactly as stipulated.

Wherever possible, the reference should be provided by an individual; however references from the organizations firm may also be accepted. Additional validation may be required where the reference is not from a named individual. The signed reference must be submitted as an electronically signed .pdf as part of the online application process with the final signed documentation pack.

To meet the requirements for the Professional Reference, an applicant organization is expected to:

- Submit the Professional Reference in electronically signed Adobe .pdf format, ensuring it has been saved according to the naming conventions stipulated by the CIF; and
- Enter the details of the professional referee into the online system.

Once an application has been submitted, the professional status of the named referee will be verified via online resources or register checks (e.g. the Law Society for registered solicitors) or other methods as deemed suitable by the CIF.

## Provision of Adobe Electronic Signature File

It is a requirement of the CIF that all documentation is electronically signed and provided in pdf format using a suitable Adobe program. See the HowTo guide within "Document3: Guidance for Cloud Service Providers" for detailed instructions on how to sign documents electronically.

Following signature of all files, applicants must make the exported signature file available to the CIF in order to validate the signature on the files.

Signature files must be sent to [adminsc@cloudindustryforum.org](mailto:adminsc@cloudindustryforum.org) once the application has been submitted. Upon submission of an application, the signature file will be used to validate all submitted and signed .pdf documentation.

## Improve

If any non-conformances are noted in the Assess step, then improvement actions are undertaken at this stage. After this, the assessment should be repeated to the extent required to ensure that all non-conformances have been corrected.

When remediating gaps, the Assessment Spreadsheet can again be used as a control schedule for improvements. If a Code requirement is inappropriate for the CSP, it is possible to request a formal Exemption from the CIF.

## Declare

The Declare Stage involves completion of the online assessment form and submitting the formal application for recognition of self-certification to the CIF.

Organizations who have used the Assessment Spreadsheet can transfer information e.g. document references, into the online system. Existing information entered at the time of registration can be reviewed for accuracy and corrected at this time. CSPs must ensure that the public disclosures webpage is live on their website(s) prior to submitting their application.

In order to prepare declarations, the organization must obtain a signed Professional Reference from a registered professional services agent, reproduced according to wording stipulated by the CIF. The Team Leader should also obtain executive management approval of the Management Declaration (also stipulated by the CIF) and ensure that they understand that they will be required to acknowledge this by email after submission of the application.

At this stage, the organization must prepare, electronically sign and upload its supporting documentation to the online system. Once complete, the application can be submitted.

## Questions to answer before moving to the next step of the Self-Certification Process:

- **have you informed the responsible Executive that they are required to return the Management Declaration via email to the required email address?**
- **have you prepared for potential rework or correction of non-conformances, which may be identified by APMG during validation?**
- **In the event that the application is successful:-**
  - **have you prepared resources to make the necessary updates to publically disclosed information (websites with logos and text)?**
  - **have you considered how you will leverage the self-certification in your promotional activities, in order to gain maximum value from your Self-Certification?**



## Validate

The CIF's appointed independent Certification Partner, APMG will validate the Self-Certification application made by the organization.

This validation will include the following checks:

1. Completeness of application
2. Digital signatures on supporting documentation
3. That publicly declared information is available on the organizations website(s) and is accurate
4. The supporting documentation covers all Code requirements, and expected content of the document type e.g. policy, procedure, professional reference etc., is found. Note: management system documentation checks will not validate the quality of the system. If a full audit is conducted, then this would be considered.
5. The identity of the professional referee either on publically available registers or by making contact with the named individual.

At the validation stage further information may be requested up to a full audit, and feedback will be provided where non-conformances are identified to give the CSP an opportunity to address them.

## Authorize

If successfully validated, APMG will formally recognize the Self-Certification on behalf of the CIF and issue a certificate confirming the certification term, together with a "Logo Pack" including the current version of the Certification Mark and detailed instructions for use.

The CIF Self-Certification website will also be updated to list the organization as certified.

## Publish

This is the final stage of the Self-Certification process as stipulated by the CIF.

At this stage, an organization who has had their Self-Certification validated and authorized is expected to display on its own website the Code of Practice Certification Mark hyperlinked to the CIF Self-Certification website pages which include details of its certification scope, together with other updates to the information on the organizations public disclosures page.

Further information on the specific requirements can be found in Document 3: Guidance for Self-Certification and the Logo Pack issued upon Authorization.

## Next Steps

Once the Self-Certification steps have been completed and the organization has achieved Certified status, they will be required to maintain their certification in order to continue to use the CIF Certified Mark.

Self-Certification lasts for 1-year, meaning an organization will need to renew the Self-Certification again at the end of this term.

Information on the Renewal process can be found in "Document 1: An Executive Briefing", and further details and guidance will be issued to certified CSPs towards the end of the certification term to support them through the Renewal process.

## Further information About the Cloud Industry Forum (CIF)

The CIF was established in direct response to the evolving supply models for the delivery of software and IT services. Our aim is to provide much needed clarity for end users when assessing and selecting Cloud Service Providers based upon the clear, consistent and relevant provision of key information about the organization, its capabilities and its operational commitments.

We achieve this through a process of Self-Certification of vendors to a Cloud Service Provider Code of Practice requiring executive commitment and operational actions to ensure the provision of critical information through the contracting process. This Code of Practice, and the use of the related Certification Mark on participants' websites, is intended to promote trust to businesses and individuals wishing to leverage the commercial, financial and agile operations capabilities that Cloud-based and hosted solutions can provide.

**For further information about the Cloud Industry Forum, please refer to [www.cloudindustryforum.org](http://www.cloudindustryforum.org)**

## Governance of The Code Of Practice

The Cloud Industry Forum has set up a governance board to be responsible for the stewardship of the Code of Practice, and full details of the board composition and committees can be found on the CIF website.

This operates independently of the CIF Management Board of the not-for-profit member body, and includes representatives from outside CIF membership, including end user representatives, industry advisors and IT legal practices to ensure a balanced and transparent approach to governance.

## Code of Practice Governance Board

The Code Governance of Practice Board is chaired by an elected representative from the governance board members, and is responsible for the following:

- Approving the CIF Code of Practice's goals, objectives and strategies in relation to the Code of Practice
- Reviewing the requirements of the Code of Practice on an annual basis and approving any changes
- Identifying the principal risks of the Code of Practice CIF CoP operations and scope and overseeing the implementation of appropriate risk assessment systems to manage these risks.
- Reviewing and approving changes the CIF Code of Practice financial performance to ensure it operates viably.
- Monitoring participant appeals, third party complaints and operational standards and consistency associated to the operation of the CIF Code of PracticeCoP
- Assessing its own effectiveness in fulfilling its responsibilities, including monitoring the effectiveness of individual representatives
- Ensuring the integrity of the CIF Code of Practice's internal control system and management information systems.

The Board can set up committees to delegate specific responsibilities from time to time as required and the composition of such committees will be set out on the CIF website.

## Audit and Appeal

In order for the Code Self-Certification process to be credible and trusted it needs to have an appropriate enforcement model to challenge any false submissions.

These validations will be based upon either a random audit, external complaint or a whistle blower alert. As such the CIF will manage an audit process (directly or through accredited 3rd parties) and will have the capability and authority to enforce removal of the Certification Mark from organizations deemed not to have complied with the Code. Independent Certification will only be enabled through bodies approved and accredited by the CIF and as such the process of carrying out an Independent Certification will automatically imbue the participant with a higher degree of trust than is achieved through Self-Certification.

If an external complaint or whistle blower statement is made about a self-certified participant that questions the validity of their declaration, the participant will be allowed to know the nature of the complaint and to provide any evidence to uphold their position as self-certified to the Code. The CIF will operate a Compliance Committee to oversee complaints and decide on their validity. In the event that the Compliance Committee upholds the complaint, the self-certified participant shall have the ability to challenge the findings by appeal to the Code Governance Board. The opinion of the Code Governance Board is final and no further route of appeal is available.

The CIF Compliance Committee will acknowledge all complaints and reserve the right to publish opinions publicly. Only the Code Governance Board or its nominated representative/s will approve any public comment on complaints.

## Collaboration with Standards organizations and related Bodies

By nature of the industry, the CIF will need to operate on an international stage as the Cloud has no geographic boundary (though our legal remit will focus initially on the UK). The CIF will collaborate and endorse appropriate security and technical interoperability standards that are outside of, but complement, the Code.

The CIF participates in the activities of ISO/IEC JTC1 SC38, which includes cloud computing via participation in the corresponding committee of the British Standards Institution.



The CIF also actively cooperates with other industry bodies with similar interests. It has a formal liaison relationship with the Computer Security Alliance (CSA) and includes coverage of the CSA's Consensus Assessments Initiative Questionnaire in the CoP.

## The Role of The APM Group Limited (APMG) in supporting Certification

APMG was established in 1993 and is a global business providing accreditation and certification services. APMG has a worldwide presence, with offices in Australia, China, Denmark, Germany, India, Italy, Malaysia, the Netherlands, the UK and the US. APMG has been working with the CIF to provide the administration behind the Code of Practice scheme.

APMG have been appointed as the CIF's independent certification partner. APMG will use its independence to ensure those organizations which sign up to the Code of Practice are confident of an impartial, reasonable, consistent and professional approach to the processing of their information and assessments.

APMG will also attend the Code Governance Board to provide a direct route for feedback from applicants working through the scheme into this monitoring body.

APMG does not provide any commercial services within the Cloud and so are able to complete the assessments of organizations without any conflict of interest, protecting the integrity and confidentiality of the information provided as part of the application process

**For further information about the APM Group Limited, please refer to [www.apmgroupltd.com](http://www.apmgroupltd.com)**

## Contact Us

**Mail: The Cloud Industry Forum, Sword House, Totteridge Road, High Wycombe, HP13 6DG**

**[www.cloudindustryforum.org](http://www.cloudindustryforum.org)**

**<https://selfcert.cloudindustryforum.org>**

**Email: [info@cloudindustryforum.org](mailto:info@cloudindustryforum.org) / [servicedesk@apmgroupltd.com](mailto:servicedesk@apmgroupltd.com)**

**Telephone: +44 (0)844 583 2521 / +44 (0)1494 459 559**