The Cloud Industry Forum Cloud Service Provider Code of Practice:

Conducting the Self Certification

2

Table of Contents

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 legal advice, 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:

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

Further information or guidance can also be sought directly from the CIF (info@cloudindustryforum.org) or APMG, CIF's Independent Certification Partner (adminsc@cloudindustryforum.org).

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

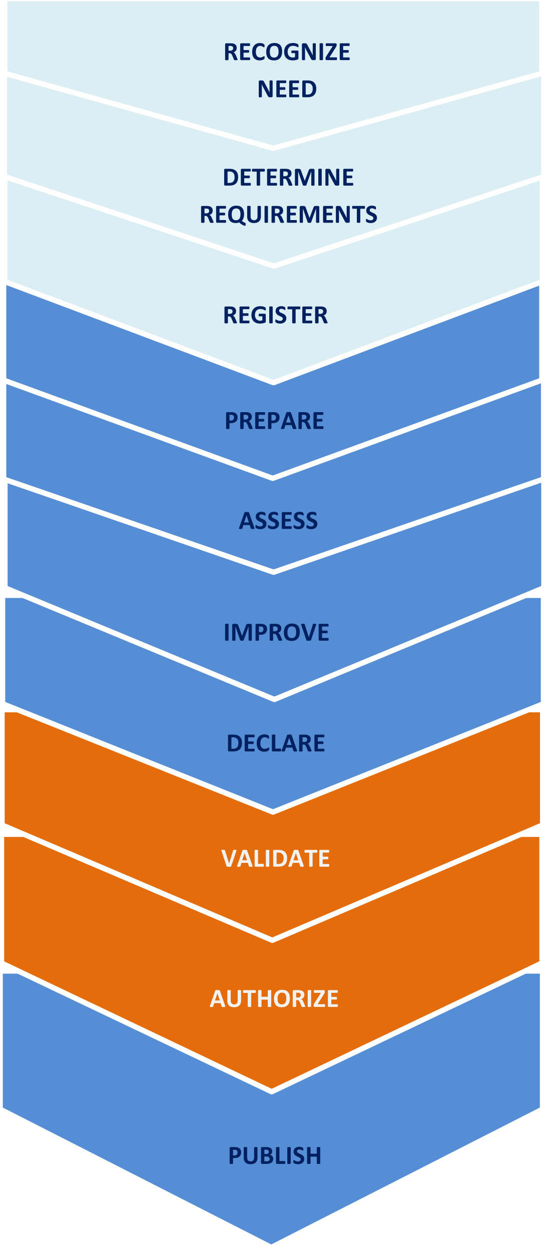
For information on the Business Case and details of how to Register for Self-Certification, refer to the following document:

- Document 1: An Executive Briefing

For additional information and instructional guidance, see also:

- Document 3: Guidance for Cloud Service Providers
- Terms and conditions

Road to Certification



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 of the CIF. The CSP must be comfortable that it is appropriately prepared for the activities involved in these stages to avoid missing the timelines for the 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. Example documents have been created and are available to download via the Self-Certification website.

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.**
- **Download, read, and ensure understanding of ALL documentation.**
- **Establish a system for organizing supporting documentation.**
- **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 address.

Assess

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

At this stage, CSP's 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.

At this stage, CSP's 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 an 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 AminSC@cloudindustryforum.org for review by the code administrators, APMG. All exemption requests will be considered on a case by case basis.

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 (V6.1.2) applicants through the Self -Certification process.

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

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 fulfil 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.

In the event of finding a false declaration or material mom-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 a press release.

What is the General Data Protection Regulation (GDPR)

The GDPR will be incorporated into UK law officially from 25 May 2018. The Government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR. The UK Information Commissioners Office (ICO) is committed to assisting businesses and public bodies to prepare to meet the requirements of the GDPR ahead of May 2018 and beyond. Whilst there may still be questions about how the GDPR would apply in the UK after leaving the EU, this should not distract from the important task of compliance with the GDPR which will be a legal requirement.

Like the UK Data Protection Act 1998 (DPA), the GDPR applies to 'personal data'. However, the GDPR's definition is more detailed and makes it clear that information such as an online identifier – e.g. an IP address – can be personal data. The more expansive definition provides for a wide range of personal identifiers to constitute personal data, reflecting changes in technology and the way organisations collect information about people.

For most organisations, keeping HR records, customer lists, or contact details etc., the change to the definition should make little practical difference. You can assume that if you hold information that falls within the scope of the DPA, it will also fall within the scope of the GDPR. With so many businesses and services operating across borders including with the use of cloud computing resources, international consistency on data protection legal requirements is crucial both to businesses and organisations.

To support the IT industry facing this legal challenge, the Cloud Industry Forum has developed its Code of Practice to enable cloud suppliers and customers to be better prepared for GDPR. The Code of Practice has integrated key themes of the GDPR in to the self-certification process, so whilst being certified does not ensure compliance to GDPR per se it is intended to offer business practical visibility and transparency of the processes from suppliers on and for customers.

More information on the GDPR is available from the ICO website at https://ico.org.uk/for-organisations/data-protection-reform/

GDPR enhancement to the Code of Practice

The majority of the requirements of GDPR will fall on the customer / the data controller. Whilst the GDPR themed additions to the Code cannot ensure compliance to the Regulation they will offer both providers and customers much greater confidence in practice that the business is proceeding appropriately towards GDPR readiness. This should help a customer choose a provider who has indicated that it has taken steps towards GDPR compliance by complying with the Code. The bulk of additions that have been made to the Code fall in to Transparency: Section A.2, entitled contracting disclosure.

There are two main types of information for pre-contract disclosure:

- Information needed by potential customers so that they can make informed decisions about relevant criteria except for capability.
- Information potentially needed during contract execution for operational purposes.

It is not the purpose of pre-contract disclosure to provide the information for an assessment of capability. The pre-contract disclosure also includes areas of transparency such as the roles of the controller and processor, geographical focus, data location and transfer of data, guarantees and remedies, complaint and dispute resolution.

Under the Capability section there are additions to personal data protection capabilities and information security management which are required to comply with personal data protection legislation/regulation and principles.

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 the 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;
- 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 process.

Optional categories of information (designated below by 'Optional'), if publicly disclosed, shall include all the types of information shown for each category. Any optional categories of information that are not publicly disclosed shall be disclosed as part of the "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 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
A.1.1 **Information for Public Disclosure**	Statement that the organization commits to complying with the Code for the scope covered by the Application (defined in A.1.3). Link to the organization's website page where publicly disclosed information is available, including statement of commitment to complying with the Code	Post-Registration Statement to be reproduced on the organization's website(s) Information to be entered into online system
A.1.2 **Corporate Identity and Responsibilities**	[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.] • Corporate name• Legal status, date of formation, location of registration, and registration number• Ownership (major shareholders) • Members of board of directors (or equivalent body) • Executive management (CEO and CFO or equivalents)• Corporate fixed address [not a post office (PO box)]	Information to appear on the organization's website(s) Information to be entered into online system
A.1.3 **Scope Covered by the Code**	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. • Scope of services• Geographical scope• Countries with local sales and/or support• Countries where customer data may be held or processed• Statement about whether the customer can restrict the countries where customer data may be held or processed	Information to appear on the organization's website(s) To be entered into the online system via free text and drop down selection
A.1.4 **Public Branding**	[Note: The information in this section is only for the scope of services covered by the Code].• Alternative trading name(s) if different [Any alternative marketing or trading ('doing business as') names]• Website address(s) [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.]	Information to appear on the organization's website(s)Information to be entered into online system

	Code of Practice Requirement	Evidence of Compliance
A.1.5 Third Party Coverage Transparency	Statement about the extent to which the organization accepts indirect responsibility for the organization’s suppliers.	Information to appear on the organization’s website(s) Information to be entered into online system
	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.	
	Statement about the extent to which the organization’s suppliers accept indirect responsibility to the organization’s customers.	Information to appear on the organization’s website(s) Information to be entered into online system
	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?	
	Statement about extent to which the organization accepts indirect responsibility to customers of customers	Information to appear on the organization’s website(s) Information to be entered into online system
	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	
A.1.6 Security Control Transparency with the Cloud Security Alliance	Statement about whether the organization has completed the Consensus Assessments Initiative Questionnaire from the Cloud Security Alliance (https://cloudsecurityalliance.org/cai.html), 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”.	Information to appear on the organization’s website(s) Status to be confirmed via online system (Yes/No checkbox)
A.1.7 Other Extended Commitments to Code of Practice Principles	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.	Information to appear on the organization’s website(s) Information to be entered into online system
A.1.8 Technological Commitments	Optional disclosure location (public or private): Statement about whether there are any specific technologies, standards, or inter-operability’s which the organization commits to supporting. 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. Reference to where relevant information about the technology, standard, or interoperability can be obtained.	Information to appear on the organization’s website(s) OR Information to be submitted with documentation provided in support of section A.2. Information to be entered into online system

	Code of Practice Requirement	Evidence of Compliance
A.1.9 Existing Certifications	Optional disclosure location (public or private): • List of any existing relevant certifications e.g. ISO 9001, ISO/IEC 27001, PCI DSS, SAS 70, SSAE 16/ISAE 3402 and Cyber Essentials. • Statement of scope of business covered by Certification, and how it corresponds to scope of Code. • By whom certification was performed, if independently certified.	Information to appear on the organization's website(s) OR Information to be submitted with documentation provided in support of section A.2. Information to be entered into online system
A.1.10 Industry Association Membership (optional)	Disclosure of this information is fully optional, however if this information is disclosed, the following should be confirmed. • List of any industry associations in which the organization has a membership. • Reference to the organization's website.	If disclosed: Information to appear on the organization's website(s) OR Information to be submitted with documentation provided in support of section A.2. Information to be entered into online system

A.2 Information for Pre-Contract 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 the required information as specified in section A.2., which may become a base document to be modified as required for prospective customers.

Additional documents may also be referred to and provided e.g. T&C’s, price sheets, user’s 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 APMG, the CIF’s 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, ensure all files have been saved per the naming conventions stipulated; and
- Confirm that each requirement area has been met via the online system

See Evidence of Compliance Column below for further details.

	Code of Practice Requirement	**Evidence of Compliance**
A.2.1 - Cloud Data Processor (CDP) identity and contacts **Updated in line with the GDPR.**	• State the CDP name, address, place of establishment, and company registration details • Specify how to contact the Data Protection Officer or other individual authorized to oversee personal data protection. • Specify how to contact a local representative for the CDP if the CDP is established in a country outside the area covered by the relevant legislation	Prototype contracting disclosure document OR Example agreement/contract PLUS Any additional supporting documentation (as required.) Documentation to be electronically signed and uploaded to the online system
A.2.2 - Customer, services and security provisions offered, and optional provisions **Updated in line with the GDPR.**	• State the nature of organisations this service is being offered to. • Describe the cloud services you offer. • Identify the types of personal data for which the offered services should not (or should) be appropriate. • Describe the level(s) of availability to be provided with the cloud services offered. • Describe the portability provisions available with the cloud services being offered.	
A.2.3 - Controller and processor roles **Updated in line with the GDPR.**	• Specify, for the service being supplied, the organization which is intended to have the controller role, with its associated responsibilities. • Specify, for the service being supplied, the organization which is intended to have the processor role, with its associated responsibilities. • Specify, for the service being supplied, whether there is any intent to have a co-controller relationship.	

	Code of Practice Requirement	Evidence of Compliance
A.2.4 - Geographical focus **Updated in line with the GDPR.**	• State the geographies where this cloud service is available to be contracted. • List the regulation(s) which govern the handling of the data protection aspects of the services you are offering. • Specify which is understood to be the competent Data Protection Authority based on where the controller is located. • Specify which is understood to be the competent Data Protection Authority based on where the processor is located.	Prototype contracting disclosure document OR Example agreement/contract PLUS Any additional supporting documentation (as required.) Documentation to be electronically signed and uploaded to the online system
A.2.5 - Data location and transfer **Updated in line with the GDPR.**	• Provide a comprehensive list of countries where personal data may be processed in any way ('personal data location'). This includes where data may be transmitted, stored, mirrored, backed-up, recovered, and provided with support. [It is not necessary to specify what functions are performed where.] • If the personal data locations may be countries covered by different data protection legislation, indicate the legal ground for transfer of personal data where not directed by or consented to by customer in contract: e.g., adequacy decision, model contracts / standard contractual clauses, Binding Corporate Rules (BCR), or any successor to Safe Harbor. • Indicate whether a customer can restrict the countries for personal data location	
A.2.6 – Subprocessors **Updated in line with the GDPR.**	• Identify all types of tasks to be performed by subprocessors that are expected to participate in the processing of the customer's personal data. NOTE: It is not required to identify subprocessors by name. • Optionally, instead of the preceding requirement, identify all subprocessors, to all levels, providing name, types of tasks performed and countries where the data may be processed. • Explain whether and how consent is given by the controller to the Cloud Data Processor (CDP) for the use of subprocessors. In particular - is blanket approval given in the contract, or is specific approval required as the changes are proposed?	
A.2.7 - Instructions, monitoring and audit **Updated in line with the GDPR.**	• Explain how the customer-data controller can issue its instructions to the CDP. • Explain what information or mechanism is available to the customer in terms of auditing or oversight to ensure that appropriate privacy and security measures described in the Data Protection Code are met on an on-going basis. • Indicate whether and what independent third party audit information will be provided to the customer, their scope, the frequency at which this information will be updated, and whether the full audit report or a summary of the report will be provided to the client. • Indicate whether the third-party auditor can be chosen by the customer or chosen by both parties and who will pay for the cost of the audit.	

	Code of Practice Requirement	Evidence of Compliance
A.2.8 - Support for controller's data protection responsibilities **Updated in line with the GDPR.**	• Explain how the CDP will support the data controller for its requirement to demonstrate compliance with applicable data protection provisions: e.g., to enable the controller to demonstrate that it has taken appropriate steps to guarantee the exercise of data subjects' rights (right of access, correction, erasure, blocking, and opposition). • Describe how the CDP, on the instruction of the controller, will make available the information necessary to demonstrate how the CDP has met its requirements related to processing. In particular - will the information be accessible on demand (e.g. via a portal), or will it need to be requested in advance?	Prototype contracting disclosure document OR Example agreement/contract PLUS Any additional supporting documentation (as required.) Documentation to be electronically signed and uploaded to the online system
A.2.9 - Guarantees and remedies **Updated in line with the GDPR.**	• Specify what guarantees the CDP offers to the controller in respect of the technical security measures and organizational measures governing the processing of personal data. • Explain what contractual remedies are available to the cloud controller in the event the CDP – and/or the CDP's subprocessors – breaches its obligations under the DP Code.	
A.2.10 - Complaint and dispute resolution **Updated in line with the GDPR.**	• Provide the contact details of the CDP representative/office who will receive questions or complaints regarding the CDP's personal data handling practices, and response timeframes. • Provide the contact details of the third party, if any, which may be contacted in order to assist in the resolution of a dispute with the CDP regarding the CDP's personal data handling practices, such as an arbitration or mediation service.	
A.2.11 - Contractual safeguards **Updated in line with the GDPR.**	• Provide the reference to, and wording of, the proposed contractual term which stipulates that the cloud data processor shall act only on instructions from the controller. • Provide the reference to, and wording of, the proposed contractual term which stipulates the obligations of the controller to ensure security of processing personal data covered under and specified in the contract, shall also be incumbent on the processor. • Provide the reference to, and wording of, the proposed contractual term which stipulates, for any processing of personal data which is subcontracted, that the processor shall choose a subprocessor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with these measures.	

	Code of Practice Requirement	Evidence of Compliance
A.2.12 - Scope covered by supporting certifications **Updated in line with the GDPR.**	Provide the following details about any certifications performed by independent third party certification bodies which are being used to provide support for some or all of the capability requirements of this DP Code. • Certification • Certification body • Start date of certification • End date of certification • Scope of certification (as stated by certification body) • Explanation of what part of DP Code capability requirements are covered by the scope of the cited certification as audited • Explanation of any part of DP Code scope not covered by the scope of the cited certification as audited.	Prototype contracting disclosure document OR Example agreement/contract PLUS Any additional supporting documentation (as required.) Documentation to be electronically signed and uploaded to the online system
A.2.13 - Commercial Terms	Pricing policy (basis of charging with fully-declared costs) • Payment terms • Contract lengths and options for discount for longer commitment • Termination basis, terms and conditions • Renewal and amendment terms and process	
A.2.14 - Personnel Profile	• Number of full-time personnel by band: (1-10, 11-50, 51-200, 201-1000, 1000+) • Number of staff based outside of the defined territory by band: (1-10, 11-50, 51-200, 201-1000, 1000+) • Employee vetting procedures undertaken	
A.2.15 - Customer Migration Paths During Contract Execution	• 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) • Ability to retrieve data in such situations	
A.2.16 - Licensing Provisions	• Who is responsible for any software/IP licensing, and any costs involved which are not covered within the cost of the services being provided? • Whether there are any licensing implications in addition to cost, including in particular whether *General Public License (GPL) is used potentially requiring publication of all code whether original code modified or not	
A.2.17 - Provisions for Information Security	• Overview of measures in place to provide for information security in general	
A.2.18 - Provisions for Service Continuity	• Overview of measures, including redundancy, to provide for service continuity including protection against data loss	
A.2.19 - Service Dependencies	• Clarification of any sub-contracting or co-location relationships (names may or may not be given) • Implications of service dependencies for service levels • Compliance with data protection requirements • Continuity of operations	
A.2.20 - Complaints and Escalation Procedures	• Complaint procedures • Escalation procedures and named individuals for escalation	

	Code of Practice Requirement	Evidence of Compliance
A.3.1 - Personal Data Breaches **Updated in line with the GDPR.**	• Inform the Cloud Data Controller on a timely basis about personal data breaches related to personal data being processed for the customer, including by any subprocessors.	Prototype contracting disclosure document OR Example agreement/contract PLUS Any additional supporting documentation (as required.) Documentation to be electronically signed and uploaded to the online system
A.3.2 - Changes of Subprocessors **Updated in line with the GDPR.**	• Inform on a timely basis about planned and actual introductions of new types of processing tasks to be performed by subprocessors. • Optionally, if provided for contractually, inform on a timely basis about planned and actual changes of subprocessors, providing the same level of detail as specified in A.2.6.2 Pre-Contract Disclosure.	
A.3.3 - Other Changes Potentially Reducing Personal Data Protection Capability **Updated in line with the GDPR.**	• Inform on a timely basis about planned and actual changes that may materially reduce personal data protection capability, including for subprocessors.	
A.3.4 - Audit Results **Updated in line with the GDPR.**	• Provide on a timely basis copies of relevant audit results for the CDP itself and for any subprocessors.	

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 the 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 referred to by organizations seeking general guidance. Area's B.5 – B.8 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 AXELOS.)

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 9001:2015 or ISO/IEC 27001:2013. 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 as per 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.

	Code of Practice Requirement	Evidence of Compliance
B.1 - Information Security Management	The specific areas for which documented management systems are required for the Code are: - 1. Written Policies: 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 must be sufficient to support the objectives of the company. 2. Written Procedures: These may include work instructions, flow charts, service/operational level agreements; third party contracts; workflows built into management applications etc. 3. Specific Individuals assigned with relevant responsibilities: These can be evidenced via organization charts, person specifications, job descriptions, RACI Responsibilities for these areas etc. 4. Appropriate training and awareness programs: These may take the form of training plans or communications to others for awareness e.g. meeting minutes, internal memos etc. 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.	ISO/IEC 27001 certificate plus scoping statement CIF Code of Practice (CoP) self-certified partner certification plus scoping statement
B.2 - Service Continuity Management		BS 25999 certificate plus scoping statement CIF CoP self-certified partner certification plus scoping statement
B.3 - Service Level Management		ISO/IEC 20000-1 certificate plus scoping statement CIF CoP self-certified partner certification plus scoping statement
B.4 - Supplier Management		ISO/IEC 20000-1 certificate plus scoping statement ISO 9001 certificate plus scoping statement CIF CoP self-certified partner certification plus scoping statement
B.5 - Software License Management		ISO/IEC 19770-1 certificate plus scoping statement CIF CoP self-certified partner certification plus scoping statement
B.6 - Complaint Handling		ISO 9001 certificate plus scoping statement CIF CoP self-certified partner certification plus scoping statement
B.7 - Environmental Impact Management		ISO 14001 certificate plus scoping statement CIF CoP self-certified partner certification plus scoping statement
B.8 - Data Protection Policy Document **Updated in line with the GDPR.**		Prototype contracting disclosure document OR Example agreement/contract PLUS Any additional supporting documentation (as required.) Documentation to be electronically signed and uploaded to the online system

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 publicly such as via a press release.

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 CIF investigation or audit has been notified to the organization.

The dated records to be maintained shall include:

- Copies of information for the 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
C.1 - Compliance with the CoP	Organizations which assert that they are complying with the Code shall be accountable for their compliance with the code and for their behaviour with customers. 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. 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 checks and random audits conducted by CIF itself, or its appointed agents.	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.
C.2 - 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. Complaint handling is covered by clause B.6 of the Code. The second requirement of this clause is covered by the following declaration: We are willing to agree to binding arbitration in local courts for the settlement of disputes.	Acceptance of statement /declaration via online system (checkbox)

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.

Before the online application is formally submitted, the 'Management Declaration' section will need to be completed. This will trigger the system to email the named senior executive (whose title and email address are entered in to 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" of the "Professional Reference Template" for details of the prescriptive content of the declaration. The content should not be altered by the organization of 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 as per 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 to How-to guide within "Document 3: 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 to validate the signature on the files.

Signature files must be sent to 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.

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.

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 organisation 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 has been successful: -**
  - **Have you prepared resources to make the necessary updates to publicly disclosed information (websites with logos and texts)?**
  - **Have you considered how you will leverage the self-certification in your promotional activities, 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 publicly available registers or by contacting 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 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

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 the CIF membership, including end user requirements, 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 CIF Code of Practice operations, scope and overseeing the implementation of appropriate risk assessment systems to manage these risks.
- Reviewing and approving changes to the CIF Code of Practice financial performance to ensure it operates viably.
- Monitoring participant appeals, third party complaints, operational standards and consistency associated to the operation of the CIF Code of Practice.
- 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 Code of Practice.

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 of 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.

Contact Us

- **Mail: The Cloud Industry Forum, Sword House, Totteridge Road, High Wycombe, HP13 6DG**
- **www.cloudindustryforum.org**
- **https://selfcert.cloudindustryforum.org**
- **Email: info@cloudindustryforum.org**