The Cloud Industry Forum Cloud Service Provider Code of Practice

An Executive Briefing

1

CLOUD
INDUSTRY
FORUM

supported by

Table of Contents

The CLOUD INDUSTRY FORUM and CIF words and associated logos are trademarks. © Cloud Forum IP Limited 2017.
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 1) is aimed at organizations interested in the Cloud Industry Forum (CIF) Cloud Service Provider (CSP) Code of Practice (Code) who may be considering or are in the process of registering for Self-Certification against the Code.

This document outlines the Business Case for seeking certification, and provides a high-level overview of the full CIF Self-Certification process, including management considerations and expectation setting, to enable a decision to be made on commitment to the Code.

Organizations should also download and refer to the following information provided by the CIF, downloadable from the CIF website www.cloudindustryforum.org:

- Document 2: Conducting the Self-Certification
- 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 APM Group, CIF’s Independent Certification Partner (servicedesk@apmgroupltd.com).

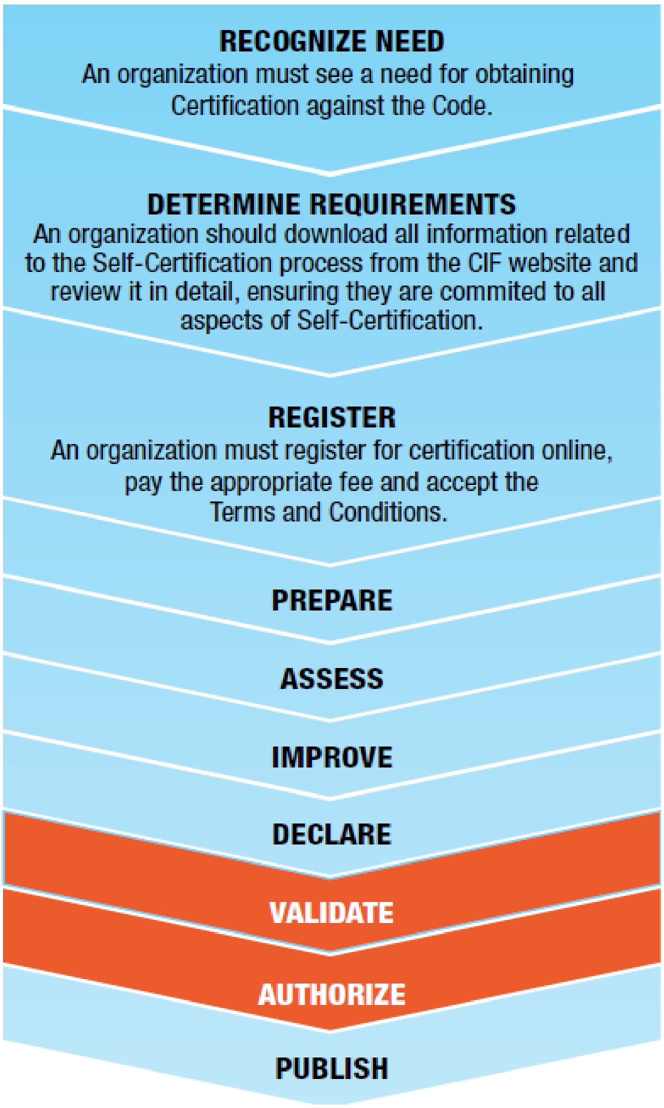
Process Stages Covered Within this Document

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

- Recognize Need
- Determine Requirements
- Register (including fees)

For information on later stages of the process, refer to the following documents:

- Document 2: The Self-Certification Scheme
- Document 3: Guidance for Self-Certification



RECOGNIZE NEED
An organization must see a need for obtaining Certification against the Code.

DETERMINE REQUIREMENTS
An organization should download all information related to the Self-Certification process from the CIF website and review it in detail, ensuring they are commited to all aspects of Self-Certification.

REGISTER
An organization must register for certification online, pay the appropriate fee and accept the Terms and Conditions.

PREPARE

ASSESS

IMPROVE

DECLARE

VALIDATE

AUTHORIZE

PUBLISH

The Need for Transparency and Trust in the cloud

Cloud computing is IT's most hyped topic at present, with good reason: the benefits which it can deliver are significant, in particular flexibility and cost savings. Furthermore, it can be a great leveller of the business playing field, virtually eliminating the high bar to smaller organizations of creating and maintaining their own IT infrastructures. As a result, it can be a driver to significant economic growth overall.

The latest research across 250 UK End User organizations in 2012 has shown that 61% of those surveyed had already consciously adopted at least one cloud service and due to their very high satisfaction levels with these services (92%), over three quarters (76%) will increase their investment in cloud solutions within 12 months. Out of those surveyed, only 4% said they had no plan to adopt cloud services as part of their IT strategy, which contrasts with the 77% who see cloud as part of their IT strategy.

Whilst the results of this survey indicate that there has been a 27% growth rate of cloud adoption over the last 18 months, there are still some significant issues raised about cloud computing that need to be proactively resolved to further increase its adoption.

Data concerns are typically the most reported upon, relating to security (preventing illegal access); privacy (ensuring no unintended access and use by third parties); and sovereignty (ensuring data is stored in a jurisdiction that is acceptable to the customer). There are other issues relating to availability of sufficient network bandwidth, capability for continuity of operations, as well as interoperability and data migration. The key point here is that these issues are long-standing issues for IT generally, not cloud specifically. However, the business imperative behind cloud computing has created the demand for clarity as to how these issues are resolved when a third-party provider is involved in the delivery of IT solutions.

Two aspects of this situation create particular issues for transparency and trust:

Lack of transparency

There are many potentially complex issues which can affect an organization's decision about a cloud computing supplier. It is typically difficult to obtain consistent and comparable information about these solutions from potential suppliers to aid a rational and informed decision. For smaller organizations, which typically do not have extensive in-house IT skills and budgets, this presents a particular exposure and challenge.

Lack of trust

There is intrinsically less basis for trust in cloud-based service providers than for traditional 'bricks and mortar' businesses as the primary relationship is usually online via the internet rather than based upon human contact, presence and relationships. For example, a poor or even fraudulent operator can quickly set up a new web-based business that looks highly professional and fully respectable, based on the infrastructure of the last failed one. How can an end user organization understand the capability and reliability of a business without an unbiased basis of review and comparison?

For more information on the findings of this research, please visit the CIF website at www.cloudindustryforum.org.

The Code of Practice Solution

The CIF (Cloud Industry Forum) was formed by organizations that recognized these business issues and identified a way to address them effectively, particularly for the smaller business. This solution was not intended to solve the underlying technical issues, nor to guarantee the performance of CSPs. The objective was to create a more level playing field for organizations doing business in the cloud, to allow consumer organizations to make better-informed decisions about the choices available.

The solution is a Code of Practice for CSPs (the 'Code'). There are core elements of focus to the Code that collectively provide relevant, focused information from which an end user should be able to make an informed decision to select a vendor that meets their operational needs:

Transparency

Organizations complying with the Code shall ensure transparency for specified types of information, some of which should be publicly available (e.g. ownership, board, executives) and some of which should be provided as part of proposals (e.g. migration paths, licensing, and provisions for data protection and continuity of operation). Commercial terms in particular, must be clear, including full disclosure of fully burdened pricing, contract periods, and renewal processes.

Capability

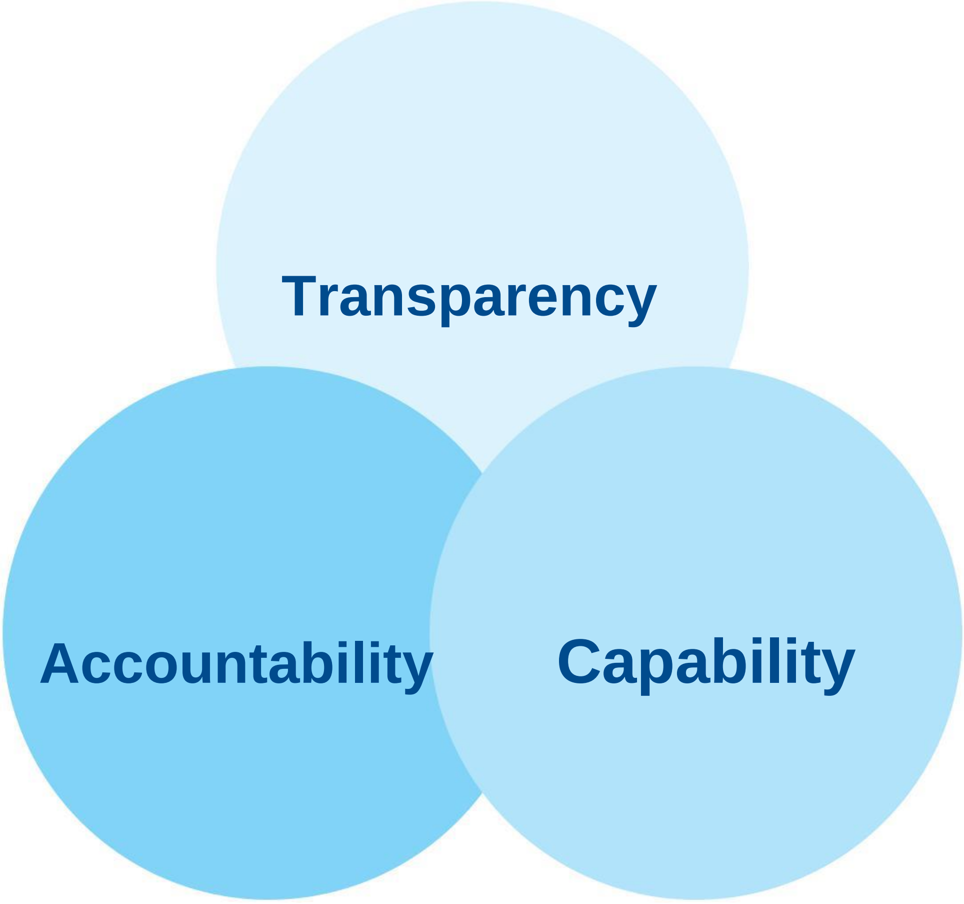
Organizations complying with the Code shall have documented management systems and resources in place to deliver specified capabilities such as data protection and continuity of operations.

Accountability

Organizations complying with the Code shall be accountable for their conformance with the Code and shall agree to binding complaint resolution procedures with customers for Code-related practices and other complainants.

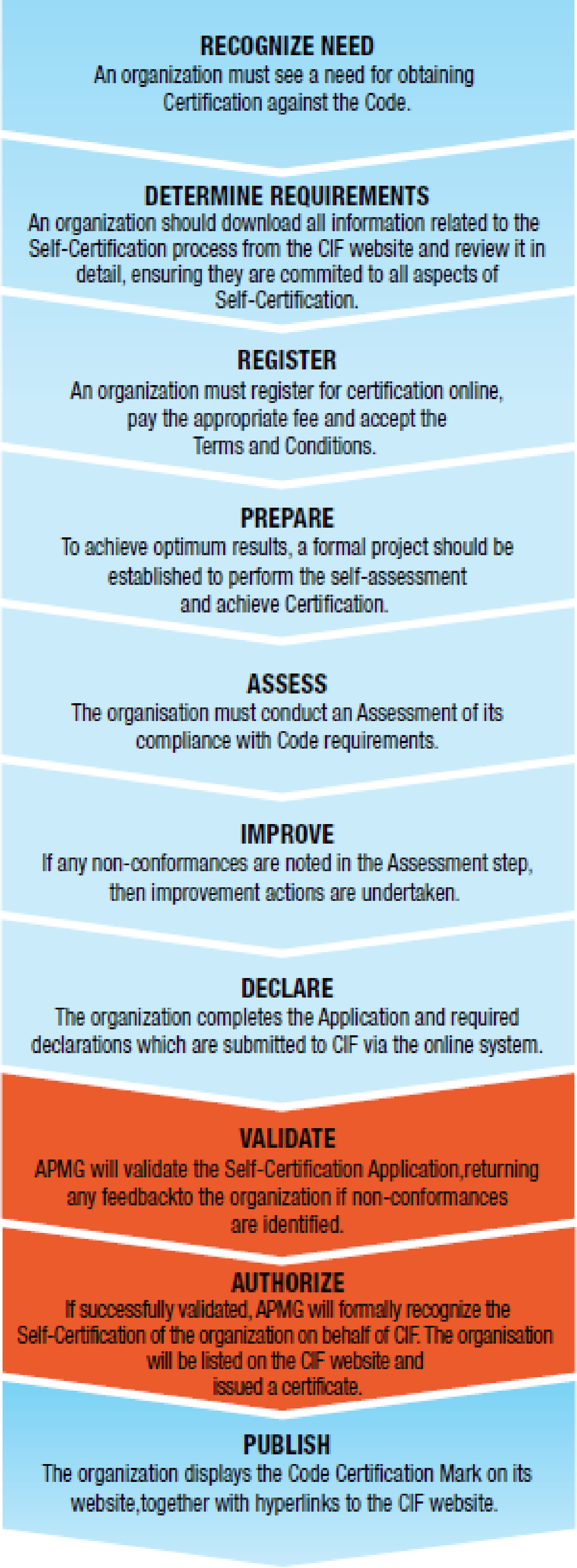
There are several different perspectives on the Code:

- Cloud Service Provider View. This is the perspective of the organization which subscribes to the Code and which is certified as complying with the Code.
- Cloud Service Customer View. This is the perspective of the organization that purchases cloud services from CSPs. The Code is intended to help these organizations make more informed business decisions about doing business in the cloud.
- CIF Member View. Because CIF is a membership-based, not-for-profit organization, its focus and activity is driven by its membership. Support from CIF members has created the Code and its supporting infrastructure. A CSP does not need to be a member to be certified.



The Self-Certification Process

The following diagram shows the end-to-end process for Self-Certification against the Code. Those items in red are validation activities performed by CIF via APM Group (APMG), its independent certification provider:



RECOGNIZE NEED
An organization must see a need for obtaining Certification against the Code.

DETERMINE REQUIREMENTS
An organization should download all information related to the Self-Certification process from the CIF website and review it in detail, ensuring they are commited to all aspects of Self-Certification.

REGISTER
An organization must register for certification online, pay the appropriate fee and accept the Terms and Conditions.

PREPARE
To achieve optimum results, a formal project should be established to perform the self-assessment and achieve Certification.

ASSESS
The organisation must conduct an Assessment of its compliance with Code requirements.

IMPROVE
If any non-conformances are noted in the Assessment step, then improvement actions are undertaken.

DECLARE
The organization completes the Application and required declarations which are submitted to CIF via the online system.

VALIDATE
APMG will validate the Self-Certification Application,returning any feedbackto the organization if non-conformances are identified.

AUTHORIZE
If successfully validated, APMG will formally recognize the Self-Certification of the organization on behalf of CIF. The organisation will be listed on the CIF website and issued a certificate.

PUBLISH
The organization displays the Code Certification Mark on its website,together with hyperlinks to the CIF website.

Self-Certification: The Business Case

Recognize Need

An organization must see a need for obtaining Certification against the Code. Typically, this will be because it wishes to differentiate itself from other organizations that do not operate transparently and responsibly. It may also be driven by customer demand or a desire from the organization to improve internal quality. It will also be possible to enquire about the Code from industry sources, e.g. by doing web searches or by reference to industry research organizations.

Cloud solutions represent the most significant development in the delivery of IT in a generation, offering end users the three-fold benefits of reduced costs, enhanced operational availability and on-demand scalability. Furthermore, Cloud technology levels the playing field for all IT consumers enabling them to participate regardless of size due to the unique pay-as-you-consume financial model, enabling SMBs to access the same technology and gain the technical agility that has previously been the reserve of large enterprises. This shift is expected, in turn, to increase market competition and innovation.

This expected market enablement and breadth of potential consumers is why leading analysts are forecasting significant growth rates over the coming years. Gartner cites market growth at 34% per annum through 2013 culminating in a market worth $150 billion worldwide. IDC in turn predicts a compound annual growth rate of 26% over the five years from 2009 to 2013, rating it six times faster growing than the traditional IT market.

CIF have identified through their latest research that end user concerns, including those relating to data security and portability which may have previously been barriers to cloud adoption are now becoming “frequently-asked-questions” of CSPs instead, which is indicative of a nascent market. However, the source of these questions and concerns suggests there is an underlying lack of transparency and trust in the market, which could certainly inhibit continued adoption.

In a market of online delivery models with many new and emerging vendors, how does a potential customer get comfort that the CSP they chose to work with will provide a trustworthy, secure, stable and effective solution, which enables them to keep control of their data throughout the contract and after? These issues are at the heart of the case for a Cloud Service Provider “Code of Practice”.

The CIF Self-Certification process enables CSPs to demonstrate transparency, capability and accountability to end users. The process then enables customers to make informed decisions about what vendors offer. The use of the Certification Mark on a vendor’s website serves two clear purposes:

1. It makes a public declaration of professional and commercial intent on the part of the CSP, and
2. It provides a visual mark of recognition that engenders confidence in the end user that the organization is open and professional in its commercial activities.

Quite simply, the Code of Practice enables professional CSPs to demonstrate their ethics, practices and processes, to build trust by association with prospective customers.

Cited Benefits to Existing Self-Certified CSPs

Organizations which have already self-certified to the Code have cited the following benefits:

- Business won. Having the CIF Code of Practice Self-Certification Mark has given smaller CSPs the credibility with large customers to win business that they otherwise would have been unable to win.
- Business processes improved. Conducting the self-assessment needed to obtain the CIF Code of Practice Self-Certification Mark identified gaps in capabilities which were relatively easy to remediate resulting in business process improvement.

The Customer Experience

The purpose of the Code is to bring greater transparency and trust to doing business in the Cloud, and it is the customer experience that is ultimately the most important for achieving this.

The customer experience operates on several levels:

1. **Trust**. The Code of Practice Certification Mark gives the customer assurance that an organization meets the requirements of the Code, and it can obtain essential information necessary to make competent business decisions.
2. **Identification of Suppliers.** The Code scheme helps customers identify suppliers at the following levels:
   - The certified listing on the CIF Self-Certification website provides links leading customers to those organizations which have demonstrated this level of responsibility.
   - CSPs registered to begin the Self-Certification process can choose to be listed on the Self-Certification website, and customers may select from them as well.
   - Visitors to the Self-Certification website can "filter" information on CSPs based on scope of services, industry sector and geographical location of data centres and availability of local support to enable more informed selection of service providers.
3. **Access to Information and Guidance**. A customer can obtain the publicly-available information covered by the Code from the certified organization's web site. CIF have also developed guidance for end users (published in "An Introduction and Guide to buying Cloud Services," free to download from the CIF website) on procurement of Cloud services, which supports both end users and those CSP's advocating the Code through certification.
4. **Complaints.** Organizations that claim Self-Certification against the Code shall be accountable for their compliance with the Code and for their behaviour with customers. If a purchasing organization has a concern that a self-certified organization is not complying with some aspect of the Code, they can choose to contact the supplier themselves and raise their issues regarding their apparent non-compliance. Alternatively, they can write directly to compliance@cloudindustryforum.org with the concern, supplying contact information for CIF to follow up to discuss details.

CIF will consider all concerns raised and investigate these to the extent it considers appropriate, including the possibility of a full audit of the self-certified organization. CIF will report back to the complainant with expected timeframes for resolution and with its findings and assessment following investigation. Because of the range of issues that may need to be considered, no specific time commitment can be given for the speed of the investigation. However, it is intended that most investigations will be completed within one month, unless a full audit is considered appropriate.

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

- **Does your organization see a real business need to certify against the Code of Practice?**
- **Can your organization see the benefit or value that CIF Self-Certification can offer?**
- **Does Certification against the Code fit in with the long and short-term objectives of your organization?**

Determine Requirements

There are three major requirements for an effective CIF Code of Practice Self-Certification project:

1. Managing Expectations
2. Ensuring Adequate Preparation
3. Ensuring Effective Execution

It is important for an organization to be clear on all the requirements related to Self-Certification against the Code before making a commitment. In addition to understanding the technical requirements of the Code of Practice standard, organizations must also recognize the effort involved with management of the certification process and the commitments associated with Certification e.g. acceptance of being audited and the Terms and Conditions relating to the use of the certification and associated mark.

1. Managing Expectations

Expectations need to be properly set and managed for a Self-Certification project to be maximally successful.

Whilst the demands for CIF Code of Practice Self-Certification should not be as major as with an externally certified ISO standard, they may still be significant, particularly for smaller organizations.

Self-Certified CSPs have stated that the investment is justified, and they would recommend Self-Certification to others; however, the demands should not be underestimated. Another justification is that some organizations view CIF Self-Certification as a stepping-stone to more extensive ISO-type certification.

To help manage CSPs' expectations, CIF have gathered the following feedback from smaller organizations:

- Adobe Acrobat is currently the only package accepted to digitally sign submissions. This license cost needs to be met.
- Capability areas typically requiring improvement are for software license management and environmental impact management. There is also often a need to improve provision for training and awareness across most capability areas.
- Some organizations have used and recommended using external consultants. The CIF acknowledges this but does not formally recognize any external consultants.

Incorrect Expectation	Correct Expectation
CIF Code of Practice Self-Certification is a marketing exercise, resulting in a collection of marketing messages structured according to the Code of Practice. The project is best managed by the marketing department who will ensure the best spin is put on messaging.	CIF Code of Practice Self-Certification has strong market value, and has provided market credibility, helping CSPs win major business, but it is primarily a transparency and management system exercise. Expectation that it can be handled as a marketing exercise will likely result in frustration as applications will lack substance.
"We do everything well now, so we should be able to get a stamp of approval on our capabilities."	Most organizations identified areas in their capabilities that required strengthening, and made improvements prior to final submission as a result. They specifically see this as a benefit of Self-Certification. Anyone starting a self-certification project should expect to find areas requiring improvement where work will be needed, but business benefits will result from this.
One person can do it all.	One person is unlikely to be able to "do it all" unless it is a one-person company. Participation will almost certainly be required from multiple functional areas in the company to ensure effective balance and depth of coverage.
"We should be able to go through a simple, cloud-based, interactive process to do everything required, explaining everything as we go. After all, this is for cloud-based business."	Cloud-based interactive processes may be powerful aids to business, but have not yet replaced much of the fundamental analysis and implementation work needed in business. Significant preparation work is required, including reading and study, as well as implementation work, such as developing and publishing required public declarations. Even though the Self-Certification process is online, in practice most organizations are initially preparing everything off-line i.e. in spreadsheets, and then using the online system for final data entry and submission.

2. Ensuring Adequate Preparation

Ensuring adequate preparation is potentially easy to achieve, but in practice easy to fail. One of the most important preparation tasks is to read through all documentation. This will take time, but it will help ensure effective execution of the entire process subsequently.

The documented requirements for Self-Certification are detailed in the following, most of which are downloadable from the CIF website (at www.cloudindustryfroum.org) or via the Self-Certification website once registered:

- Document 1: An Executive Briefing (this document)
- Document 2: Conducting the Self-Certification; which includes the technical requirements (the ‘Code”)
- Document 3: Guidance for Cloud Service Providers; which includes details of how organizations should provide evidence to meet the requirements and information on downloadable templates.

It is critical that at least one individual within an applicant CSP reviews all materials and resources provided by CIF and seeks any clarification from CIF or APMG on the process or materials, as required.

For example, this document provides a high-level overview of the process to enable a decision to be made on commitment to the Code, whereas other documents are instructional, and will need to be referenced by the project team when preparing the application. The Project Manager or Team Leader should understand how and when to use all resources and guidance provided.

3. Ensuring Effective Execution

It is strongly recommended that a CSP initiates a formal project to achieve Self-Certification.

See the “Prepare” section of “Document 2: Conducting the Self-Certification” and “Document 3: Cloud Service Provider Guidance”, for more information on preparation activities.

Questions to answer before moving to the next step of Self-certification:

- **Do you understand the technical requirements in full?**
- **Do you have a realistic view of the expectations of the Self-Certification process?**
- **Can you commit to the preparation required?**
- **Have you reviewed the ‘Terms and Conditions’?**
- **Have you revisited and validated the business case and justification for Self-Certification?**
- **Have executive management approved the decision to self-certify considering the proposed course of action, fees, and commitment to investment of resources?**
- **Is there business justification to become a CIF member to drive the future development of the Code and its adoption? The Membership Pack may be downloaded from www.cloudindustryforum.org. Note that you do not need to become a member in order to become certified.**

Certification Fee

Self-Certification by nature is carried out by participants using their own resources and at their own cost. However, participants must pay a nominal fee to assist in the administration and governance of the Code to ensure its integrity is maintained - for the benefit of the industry and the market. The Annual Self-Certification fee is due at registration or renewal, and is charged on the following basis:

Organization with turnover	Annual Fee (excl. VAT or other taxes)
Up to £1m	£700 per annum
£1m to £5m	£1750 per annum
£5m to £10m	£2500 per annum
£10m to £25m	£3000 per annum
£25m to £100m	£6000 per annum
Over £100m	£9000 per annum

The fee must be paid during Registration (or Renewal) via the online system using a valid Credit or Debit Card, PayPal account, or invoice and is non-refundable. CSPs must ensure they meet any payment terms stipulated when choosing to pay by invoice. Failure to do so may result in organizations needing to register again.

Submission of the Self-Certification application must be made within six months of the registration date or the registration will lapse. A new fee will be payable to re-register.

Additional Considerations

The following information should also be considered by organizations who wish to undertake Self-Certification against the Code.

The Audit Experience

If the CIF decide to perform an audit of a CSP for compliance with the Code, the following will typically happen:

- Notification. CIF notifies the organization about the audit, and requests confirmation of dates and logistical arrangements for an on-site visit. Where non-conformance is suspected based upon 3rd party claims, the on-site visit will likely occur in a shorter time-frame than for other audits or spot checks usually within 21 days of notification. In other cases, it must occur within 45 days of notification within 21 days of notification. In other cases, it must occur within 45 days of notification.
- Offsite Review of Application and Supporting Documentation. CIF (via its nominated auditors) will review the application and supporting documentation for compliance with Code requirements.
- Onsite Review. The CIF (via its nominated auditors) will conduct an on-site review to validate compliance, with respect to adequate disclosure of non-public information in all commercial proposals; and evidence of proper operation of documented management systems required by the Code.
- Report. The auditor(s) will prepare a report of findings to the CSP within seven working days from the end of fieldwork.
- Management Response. The CSP has seven working days to provide written management responses to the report.
- CIF Action. Depending on the results of the audit and the management responses, the CIF may take any action it deems appropriate up to and including public rescission of the Certification including the immediate and unilateral withdrawal of permission to use the Certification Mark.

If the result of an audit is a finding that the organization has not complied fully with the Code, the CSP may be liable for the costs of the Audit.

The Renewal Experience

Renewal is similar to the original Self-Certification experience, except for the following key differences:

- The CIF will remind an organization approximately three-months before the anniversary date of their initial certification about the need to perform a renewal Self-Certification.
- Prior to renewal, CSPs should determine the value the certification has offered and should ensure they see continuing value in holding Certification against the Code. Organizations can remind themselves of the need to be certified by reviewing this document again in full, and by seeking further guidance or information from market and industry sources. CSP's may also contact CIF for information on their PR activities and efforts to promote the value of and need for a CSP Code or Practice.

CSPs should again consider the costs involved and based on these factors, decide to either withdraw from the scheme or renew their certification.

Decision to Withdraw

If an organization decides not to renew their certification they will have: -

- Five working days to remove the Certification Mark from their website(s)
- 30 days to ensure the Certification Mark is removed from marketing or any other collateral
- 30 days to provide written confirmation to adminsc@cloudindustryforum.com to confirm the above has taken place which will be subject to checks

The CIF will police this via their certification partner, APMG, and will consider taking action with any organization that is no longer in compliance with the terms and conditions relating to the use of the Certification Mark.

Decision to Renew Self-Certification

If the organization decides to renew, they will be required to: -

- Re-certify under the latest version of the Code,
- Update their online public disclosure to ensure they reflect the current situation for their organization, and
- Pay the current fee for certification (there are no separate fees for renewal) according to the organization turnover.

A 30-day grace period will be granted for late submission of renewal applications, but thereafter the organization loses the right to use the logo and will be no longer appear on the CIF website.

Once committed to renewal of an existing certification, the following process should be followed and must be completed during the three-month window from notification of expiry of existing self-certified status to enable ongoing use of the Certification Mark: -

- **Prepare.** Similar to initial certification, an organization should ensure they are adequately prepared. A formal project should be established for the Self-Assessment and existing information should be gathered in preparation for review. It is extremely important at this stage that an organization review the latest version of the Code as requirements may have changed since initial certification.
- **Assess.** The difference between assessment at renewal and initial certification is that organizations will typically be looking for changed information since the last certification application AND identifying gaps arising from changes to the Code or additional requirements as documented by the CIF. When renewing certification: -
- ***if information has changed*** - the organization must update this information which will be subject to validation checks by APMG. This would include changes to publicly disclosed information (including company contact information) as well as supporting documentation.
- ***if information has not changed*** - CIF will recognize information submitted under the previous certification term and will require an organization to submit a written, signed declaration from the Senior Representative to confirm this is the case. This declaration must be provided on the CSP's letter headed paper and declare that the information submitted under the previous certification period and be signed by the same person who submits the Management Declaration.
- **Declare**. Organizations must make their declarations via the online system. When conducting a renewal, a record of the existing certification information which is coming to the end of its annual term, will be duplicated (the original certification record will be retained) to enable editing or reconfirmation of information previously entered into the online system, as well as the upload of updated documentation as required. Documentation must again be digitally signed and the CSP will also be required to submit a new Management Declaration to confirm ongoing commitment to the Code and the Terms and Conditions.
- **Validate.** Following this, changed information and/or declarations provide in the renewal submission will be validated by APMG, who will advise of any non-conformances or success in the renewal process.
- **Publish.** Once validated, the organization will be issued a new certificate and Logo pack (if it has been updated since the last certification) and can continue to use the certification for another year.

Commitment to the Code

Once an organization has validated the Business Case and determined requirements, including costs for Self-Certification and ongoing commitments, they are ready to make a commitment to the Code through registration.

Register

An organization must register for certification online, pay the appropriate fee and accept the Terms and Conditions.

The registration process is online at https://selfcert. cloudindustryforum.org.

The following basic information is required to register, all of which can be updated when completing the full application:

- Details for primary and secondary contacts
- Corporate name - it is also possible to upload a company logo (dimensions: max 145 px by 75 px)
- Alternative trading name(s) if different
- Website address(s)
- Organization turnover range (for determination of cost)

At this stage, the scope of services to be certified should also be specified using a pre-defined list of categories for service type and geographies covered. Verticals served may also be specified. This information can also be used for customer filtering of the CIF database of listed self-certified (or registered) organizations.

A user ID and password must be specified at registration, which must be retained to re-enter the online system and complete the application.

The Terms and Conditions must also be agreed as part of the registration process.

Next Steps

Once registered for the Self-Certification process, the next steps are the detailed Assessment work.

Explicit guidance on the next steps can be found in “Document 2: Conducting the Self-Certification” and “Document 3: Cloud Service Provider Guidance”.

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 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 Practice (CoP).
- 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, 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

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 / servicedesk@apmgroupltd.com

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