UK FINANCE

CLOUD COMPUTING CONTROLS FRAMEWORK

A Procurement Framework for Public Cloud Computing Services

This report is intended to provide general information only and is not intended to be comprehensive or to provide legal, regulatory, financial or other advice to any person. Information contained in this report based on public sources has been assumed to be reliable and no representation or undertaking is made or given as to the accuracy, completeness or reliability of this report or the information or views contained in this report. UK Finance shall have no liability to any person arising from or in connection with any use of this report or any information or views contained in this report.

ABOUT THIS FRAMEWORK

UK Finance sponsored the creation of a public cloud computing framework that sets out best practice for the procurement and ongoing management of cloud computing as a service. The target audience for this framework is any financial service provider and it will be particularly helpful for the technology, risk, vendor management and procurement functions within institutions.

The controls have been derived from analysis of UK Finance members control sets and in collaboration with cloud service providers. Each control has been cross checked for compliance against ISO 27001, COBIT 5.0, Cloud Security Alliance Guidance, AICPA SOC 1 and EBA Cloud Outsourcing Guidelines.

The framework consists of 44 controls, each control is mapped to one of nine domains and one of eleven risks associated with the management of cloud computing as a service.

HOW TO USE THIS FRAMEWORK

The framework can help teams across the technology lifecycle, bearing in mind that it will depend on your individual organisation. Those working in technology procurement could use it as part of their tender process to assist in checking suppliers are following best practice, and those who work in contract management could use it as part of their ongoing supplier engagement.

Audit and risk functions could use the framework to assess the ongoing risk management profile of their public cloud estate by aligning with best practice. Those in security could use it when assessing and managing security for tools and applications (such as encryption key management).

Where applicable, available evidence should be sought from the cloud service provider to support responses.

Many thanks to the following institutions:

- Bank of America Merrill Lynch
- CYBG
- HSBC
- Lloyds Banking Group
- Royal Bank of Scotland
- Santander
- Amazon
- Google
- Microsoft

IDENTIFIED DOMAINS AND RISKS

Domains	
Audit assurance and compliance	Assuring customer institution that the provider has appropriate business continuity and operational resilience measures
Encryption key management	The processes, and their management, used to keep customer data secure and segregated from other tenants
Governance	The provider's internal policies and governance and how they may affect customer data
Identity and access management	Assuring that the appropriate controls can or will be in place to ensure the security of customer data
Lifecycle management	The lifecycle of data and how it is deleted/removed from the provider
Security controls on physical infrastructure and facilities	The physical security of the datacentres where client data and/or systems are hosted
Security of cloud networks and connections	The virtual security of the cloud infrastructure and its connections with other systems, whether customers or third parties
Security provisions for cloud applications	The virtual security of the cloud applications
Workforce security and access management	How the staff of the provider have been trained to ensure the security of customers' data

Risks
Business viability of provider
Compliance with EU regulation and legislation
Inability to audit cloud service provider in compliance with clients' internal policies and regulatory expectations
Inability to set or enforce security policy with cloud service provider
Inability to track or troubleshoot data once it leaves the client
Inability to track or troubleshoot data once it leaves the client and/or unauthorised access or leak of unauthorised data
Provider's business continuity and disaster recovery readiness
Security defects in technology
Unauthorised access or leak of customer data
Unauthorised access or leak of proprietary data
Vendor lock-in

	Domain	Control	Risk
1	Audit assurance and compliance	Do you have an independent function which periodically reviews processes and systems for compliance with policies?	Unauthorised access or leak of customer data
2	Audit assurance and compliance	Do you support forensics and investigations on your virtual infrastructure?	Inability to track or troubleshoot data once it leaves the client
3	Audit assurance and compliance	Do you have the technical and contractual capabilities in place to support such investigations?	Business viability of provider
4	Audit assurance and compliance	Will you allow us physical access to your premises in the context of audits and does your contract provide supervisory audit rights?	Inability to audit cloud service provider in compliance with clients' internal policies and regulatory expectations
5	Audit assurance and compliance	Describe how you support a customer that wants to exit the service? What technical and contractual means are in place to support this?	Vendor lock-in
6	Audit assurance and compliance	Describe your contingency plan in case a supplier or partner decides to end the relationship	Vendor lock-in
7	Audit assurance and compliance	What are your procedures for securely migrating data to other cloud platforms or back to the organisation?	Unauthorised access or leak of customer and/or propriety data and vendor lock-in
8	Encryption key management	Please detail the cryptographic key management systems in place for your cloud services, and are they governed by a defined and documented cryptography policy?	Unauthorised access or leak of proprietary data
9	Encryption key management	Please describe which encryption standards and certifications are available for the online service	Unauthorised access or leak of proprietary data
10	Encryption key management	Is data encrypted at rest and in transit in open/validated formats?	Unauthorised access or leak of proprietary data
11	Encryption key management	Do you use a hardware security module for cloud infrastructure cryptographic key management? If yes, then please answer the following question	Unauthorised access or leak of proprietary data

	Domain	Control	Risk
12	Encryption key management	Is the HSM certified against FIPS 140-2 or other standards and if so, at which level? How do you manage access and authorisation for keys and certificates stored in these HSMs, and for subordinate keys protected by the HSM keys? When operating the service, can you ensure there are no ways to bypass security provided through the HSMs when accessing lower-level encryption keys?	Inability to track or troubleshoot data once it leaves the client
13	Governance	Please describe how you govern customer data internally	Inability to track or troubleshoot data once it leaves the client
14	Governance	Are all actions in the online service audited and are these audit logs available to the customer? How long is this information stored or archived?	Provider's business continuity and disaster recovery readiness
15	Governance	Please identify the individual or group, including executive leadership and senior management, who are responsible and accountable for information security and business continuity within your organisation and detail their responsibilities	Provider's business continuity and disaster recovery readiness
16	Governance	Please outline your disaster recovery and business continuity plans and any relevant testing	Inability to audit cloud service provider in compliance with clients' internal policies and regulatory expectations
17	Governance	Are your information security policies made available and communicated to staff and contractors?	Inability to audit cloud service provider in compliance with clients' internal policies and regulatory expectations
18	Governance	Are there procedures in place to ensure policies are reviewed by staff and contractors?	Inability to audit cloud service provider in compliance with clients' internal policies and regulatory expectations
19	Governance	Please explain how customer data is governed. Who can access customer data within your organisations and what safeguards are in place to control and monitor this?	Unauthorised access or leak of customer and/or propriety data

	Domain	Control	Risk
20	Identity and access management	Do you allow the use of open standards and/or identity federation standards to delegate authentication capabilities to your tenants?	Unauthorised access or leak of customer and/or propriety data
21	Identity and access management	Do you support identity federation standards as a means of authenticating/authorising users?	Unauthorised access or leak of customer and/or propriety data
22	Identity and access management	Does your information access management system solution provide for role/context-based entitlement based upon the classification of data and the principle of least privileged access?	Security defects in technology
23	Identity and access management	How do you protect access to administrative accounts that give broad access to parts of the service? Do you ensure that, at as a minimum, any accounts with full administrative privilege require multi factor authentication?	Unauthorised access or leak of customer and/or propriety data
24	Identity and access management	Are the information and operating systems protected by appropriate organisational and technical access controls, including network access control?	Unauthorised access or leak of customer and/or propriety data
25	Identity and access management	Are user credentials for physical and logical access to locations, systems and information reviewed during defined intervals and are the requirements contained within a defined documented policy?	Unauthorised access or leak of customer and/or propriety data
26	Identity and access management	Do you use generic (non-personalised) accounts and how do you manage them? Do you have policies and procedures in place to ensure that generic accounts for systems and applications are appropriately managed and monitored at all times?	Security defects in technology
27	Identity and access management	Do you have a process ensuring that the use of these generic accounts is kept to a bare minimum?	Inability to set or enforce security policy with cloud service provider
28	Identity and access management	Do you have a defined and documented password policy that mandates quality password criteria such as length, age, history and complexity, as well as global requirements for lockout enforcement and duration?	Inability to track or troubleshoot data once it leaves the client

	Domain	Control	Risk
29	Identity and access management	Are the information access management requirements for the provisioned online service clearly articulated and documented with appropriate terms?	Inability to track or troubleshoot data once it leaves the client
30	Lifecycle management	How does the deletion of data work? Is data securely deleted from, but not limited to, your data centre storage, contingency sites and backup media when no longer required?	Unauthorised access or leak of customer and/or propriety data
31	Lifecycle management	Is the process for the secure deletion of data automated (by technical policy or scheduled work) or is the process manually done by auditable process?	Compliance with EU regulation and legislation
32	Security controls on physical infrastructure and facilities	Do you have physical and logical security controls around information systems and databases to avoid unauthorised access and detect/prevent potential data leakage?	Security defects in technology
33	Security controls on physical infrastructure and facilities	What is the geographic location and legal jurisdiction of the data centre that will be storing and/or processing customer data?	Security defects in technology
34	Security of cloud networks and connections	Are your network environments and virtual instances designed and configured in accordance with a documented network security policy to restrict and monitor traffic between trusted and untrusted connections?	Security defects in technology
35	Security of cloud networks and connections	Are these configurations reviewed at least annually, and risk assessed to justify use for all allowed services, protocols, ports, and by compensating controls?	Unauthorised access or leak of customer and/or propriety data
36	Security of cloud networks and connections	Do you have documented information security baselines for every component of your cloud infrastructure? (e.g. hypervisors, operating systems, routers, DNS servers, etc.)	Unauthorised access or leak of customer and/or propriety data

	Domain	Control	Risk
37	Security of cloud networks and connections	Do you perform regular penetration testing with a CREST approved (or equivalent) penetration testing third party or individual, on your infrastructure?	Unauthorised access or leak of customer and/or propriety data
38	Security of cloud networks and connections	Do you ensure there is a log and notifications for all virtual network changes?	Unauthorised access or leak of customer and/or propriety data
39	Security of cloud networks and connections	Do you ensure that you have a log of information about IP traffic going to and from the interfaces of your virtual networks?	Vendor lock-in
40	Security of cloud networks and connections	Do you also monitor data that is entering or leaving these networks?	Unauthorised access or leak of customer and/or propriety data
41	Security of cloud networks and connections	Are all DNS services used for the corporate and production environments secured in accordance with good practice, and monitored to detect access and changes?	Unauthorised access or leak of customer and/or propriety data
42	Security provisions for cloud applications	When applicable, does your Hardware Security Module (HSM) or HSM as a service include cryptographic mechanisms to support secure logging of transactions, data, and events to enable auditing?	Inability to audit cloud service provider in compliance with clients' internal policies and regulatory expectations
43	Security provisions for cloud applications	How do you encrypt information through the data lifecycle (create, store, transmit, process, archive, backup, destroy)?	Inability to track or troubleshoot data once it leaves the client and/or unauthorised access or leak of unauthorised data
44	Workforce security and access management	Do you conduct security training for the relevant staff with appropriate procedures for reporting and acting on unauthorised activity and misuse of confidential information?	Unauthorised access or leak of customer data

OUR TEAM

Dan Crisp, Director, Digital, Technology and Cyber, UK Finance

Dan is the Director for Digital, Technology and Cyber at UK Finance, overseeing policy initiatives including FinTech, cloud computing and data protection. Dan is also focused on projects to operationalise industry utilities for technology risk and E-ID.

Prior to joining UK Finance, Dan was the Chief Operations Officer for Barclays Global Information Security, primarily responsible for the technical integration of global acquisitions. Dan has also held various senior risk and compliance roles at JP Morgan and Citigroup. Most recently, Dan served as the Chief Technology Risk Officer for BNY Mellon where he led the innovation, development and deployment of global technology risk regulatory controls.

Dan is a board member for the Internet Security Alliance, a non-executive director for Huntswood and a charter member of the Cloud Security Alliance metrics group. He is also a mentor at Level 39, Europe's largest FinTech accelerator and incubator. Dan holds qualifications from the University of Memphis (USA) and Stanford University (USA). He has also completed the Strategic Management Program at Cambridge University (UK).

Ian Burgess, Head of Cyber Policy, UK Finance

Ian is the Head of Cyber Policy at UK Finance, primarily focused on operationalising the Financial Sector Cyber Collaboration Centre (FSCCC), an industry utility designed to promote cyber intelligence sharing amongst financial institutions and increase the cyber resilience of the whole sector. He also leads on cyber security regulatory or policy responses that impact UK financial services.

Most recently Ian was part of the BNY Mellon EMEA technology risk leadership team where he led on the development and deployment of a global system to map technology risk regulatory controls to global regulations and also managed the redesign of the entire suite of technology risk metrics.   Prior to this, having commissioned from the Royal Military Academy Sandhurst he served eight years as a British Army Officer, managing complex strategic communications installations and providing leadership and communications training.

Ian holds a BA (Hons) degree in Business Studies from Coventry University, and is a certified Project Management Professional (PMP), Certified Information Security Manager (CISM) and Certified in Risk and Information Systems Controls (CRISC).

Oliver Nelson Smith, Business Analyst, UK Finance

Oliver is a business analyst in UK Finance, supporting all areas of the Digital, Technology and Cyber team. Recent projects have included the business analysis for the strategy and business case of the Financial Sector Cyber Collaboration Centre, creating a comprehensive Actions and Communications tracker, mentoring interns and supporting the head of the Digital, Technology and Cyber team.

Before coming to UK Finance, Oliver had multiple experiences in hospitality, from creating a database of venues for Triumph UK, to managing teams of bar staff. He taught English Speaking in Tokyo, Japan and studied Aeronautic Engineering at the University of Southampton. He has a TEFL qualification, a Duke of Edinburgh and was a house prefect at Rugby School.

www.ukfinance.org.uk
UK Finance
1 Angel Court
London, EC2R 7HJ
United Kingdom