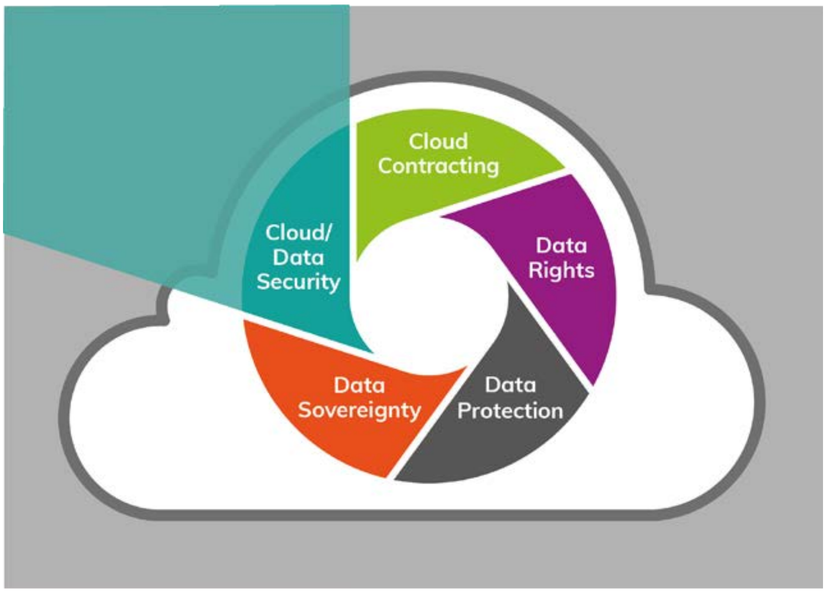
Insight and Thought Leadership Service | WHITE PAPERS

Legal Aspects of Cloud Computing: Cloud Security

Richard Kemp

June 2018



KEMP IT LAW

kempitlaw.com

21 Napier Avenue London SW6 3PS Tel 020 3011 1667 Web www.kempitlaw.com

LEGAL ASPECTS OF CLOUD COMPUTING: CLOUD SECURITY

TABLE OF CONTENTS

TABLES, ETC.

LEGAL ASPECTS OF CLOUD COMPUTING: CLOUD SECURITY[1]

A. ENTERPRISE CLOUD ADOPTION

1. **After GDPR.** After the bow wave of GDPR readiness legal work in the run up to 25 May 2018, IT lawyers may be forgiven for thinking that the biggest change is now behind them. But the truth is that GDPR heralds rather than ends a period of change in IT law and regulation as business transforms through the adoption at scale of new technology. Nowhere is this more clearly shown than in the legal aspects of the rapidly developing area of cloud security.

2. **Enterprise computing is migrating to the cloud quickly** . A central feature of this transformational change is the epic migration now well underway in enterprise (large organisation) computing from 'on premise' – traditional IT infrastructure at the user – to 'in-cloud' – open access to the public cloud, the more dedicated resources of the private cloud and their hybrid cloud combination. The development of the enterprise cloud is as significant as the migration of electricity generation out of the factory to the UK national grid in the 1930s but with many more facets, as each component of IT infrastructure – power, compute, network, memory, storage and software - gets the cloud's 'as a service' treatment.

3. **Increasing data volumes are fuelling cloud growth**. The cloud, as an extension of Moore's Law, demonstrates the marvel of compound growth, and cloud data centre economics are truly mind boggling: driven by the Internet of Things (IoT), data volumes created are growing by 30% to 40% annually, so will increase by 4x to 5x over the next 5 years. Data created is currently two orders of magnitude (100x) higher than data stored, so data stored in the cloud's data centre 'core' has some catching up to do, and in 5 years' time will be 5x to 10x higher than today.[2] At the same time, cloud power consumption rises[3] whilst everything inside the data centre gets smaller and faster: technology advances in cloud storage for example mean that storage device space - 'tin on the floor' - will reduce to a small fraction of what it is today even as data volumes stored rise exponentially.

4. **Cloud Service Providers (CSPs) are growing rapidly**. Networking company Cisco Systems in its current Global Cloud Index forecasts that by 2022 there will be over 600 of 'hyperscale' data centres globally, operated by 24 CSPs and by then accounting for over 85% of the public cloud's installed

[1] A version of this paper is shortly to be published in *The Computer Law and Security Review*

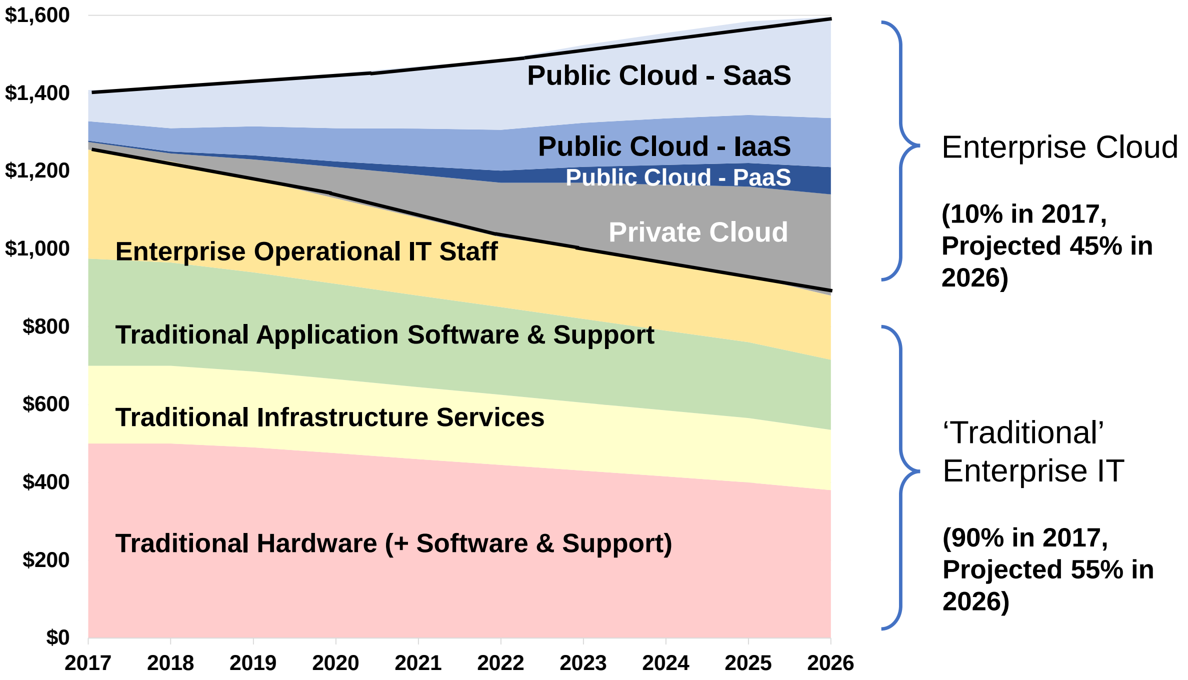
[2] See '*Data Age 2025'*, International Data Corporation White Paper, April 2017 - https://www.seagate.com/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf

[3] Data centres are forecast to use between 1,200 TWh/year (terawatt hours per year) (best case) and 3500Twh/year (expected case) of electricity within 10 years, or between 4.5% and 13% of global electricity consumption. See '*Tsunami of data could consume one fifth of global electricity by 2025'*, The Guardian, 11 December 2017 - https://www.theguardian.com/environment/2017/dec/11/tsunami-of-data-could-consume-fifth-global-electricity-by-2025 - citing '*Total Consumer Power Consumption Forecast*', Anders Andrae, 7 October 2017 - https://www.researchgate.net/publication/320225452_Total_Consumer_Power_Consumption_Forecast. For a recent example of innovative data centre technology, see '*the Orkney Islands in Scotland just became one of the most exciting places in tech*', Microsoft, 6 June 2018 - https://news.microsoft.com/en-gb/2018/06/06/the-orkney-islands-in-scotland-just-became-one-of-the-most-exciting-places-in-tech/

server base and workloads[4]. The development of the cloud is particularly visible at the moment in the cloud revenue growth of the three largest CSPs, with Amazon Web Services (AWS) increasing by 50% annually and Microsoft and Google each by around 100%: by 2020, cloud revenues at AWS, Microsoft and Google are forecast to reach $44bn, $19bn and $17bn respectively.[5]

5. **Cloud's share of enterprise IT is set to rise from 10% to 45% by 2026**. Aggregating the elements of 'traditional' enterprise computing (hardware, services, applications and staffing), comparing them to the private cloud and the Infrastructure (IaaS), Platform (PaaS) and Software (SaaS) elements of the public cloud, and projecting them all forward over the next ten years, open source IT research organisation Wikibon has forecast that the cloud's share of enterprise computing will grow from around 10% currently to 45% by 2026.[6] The chart at Figure 1 is derived from these projections.

Figure 1: Worldwide Enterprise IT Projection by Segment, 2017-2026 ($bn)



[4] '*Cisco Global Cloud Index: Forecast and Methodology, 2016-2021*' (updated February 2018) - https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.html. Cisco defines criteria for hyperscale CSPs as annual revenues of (i) >$1bn from IaaS, PaaS or infrastructure hosting, (ii) >$2bn from SaaS, (iii) >$4bn from internet, search or social or (iv) >$8bn from e-commerce or payment. Cisco identifies 24 hyperscale CSPs by these criteria, of which 17 are in the United States: Adobe, ADP, Amazon, Apple, AWS, eBay, Facebook, Google, IBM, Intuit, LinkedIn, Microsoft, Oracle, Rackspace, Salesforce, Twitter and Yahoo; and 7 are elsewhere: Alibaba, Baidu, JD.com and Tencent (China); NTT and Yahoo!Japan (Japan); and SAP (Germany).

[5] '*Cloud Revenue 2020: Amazon's AWS $44B, Microsoft's Azure $18B, Google Cloud Platform $17B*', John Koetsier, Forbes, 30 April 2018 - https://www.forbes.com/sites/johnkoetsier/2018/04/30/cloud-revenue-2020-amazons-aws-44b-microsoft-azures-19b-google-cloud-platform-17b/2/#2d079dd11b43

[6] '*Cloud "Vendor Revenue" Projections 2015-2016*', David Floyer, 28 February 2017, Wikibon - https://wikibon.com/cloud-vendor-revenue-projections-2015-2026/ - cited in '*Roundup of Cloud Computing Forecasts, 2017*', Louis Columbus, Forbes, April 29, 2017 - https://www.forbes.com/sites/louiscolumbus/2017/04/29/roundup-of-cloud-computing-forecasts-2017/#253cc79331e8

6. **Cybersecurity risks to the enterprise are also rising: the NCSC's 2017-2018 report**. Cybersecurity threats that the enterprise faces also continue to grow in range, intensity and scale.[7] The NCSC[8] in its 2017-2018 report, '*the cyber threat to UK business*' states (on page 6):[9]

> "Cyber attacks have resulted in financial losses to businesses of all sizes. The costs arise from the attack itself, the remediation and repairing reputational damage by regaining public trust. Attacks have also triggered declines in share prices and the sacking of senior and technical staff held to account for massive data breaches. The enforcement of the General Data Protection Regulation (GDPR) in May 2018 could, under certain circumstances, lead to severe fines for organisations which fail to prevent data breaches, which result in a risk to the rights and freedoms of individuals.[10]
>
> Between October 2016 and the end of 2017, the NCSC recorded 34 significant cyber attacks (that is, attacks that typically require a cross-government response), with WannaCry the most disruptive of these. 762 less serious incidents (typically confined to single organisations) were also recorded. 2018 will bring more of these attacks. The Internet of Things and its associated threats will continue to grow and the race between hackers' and defenders' capabilities will increase in pace and intensity."

Cloud security is only a part of these cybersecurity risks and threats, and it is a truism that an organisation's security is only as strong as its weakest link. The NCSC 2017-2018 report noted ransomware, DDoS attacks, massive data breaches and supply chain compromise as among major incident trends, with other significant incidents including CEO/senior executive BEC (business email compromise), major security vulnerabilities (Meltdown and Spectre in January 2018), financial sector compromise (fraud using the SWIFT payment system) and cyber crime 'as a service'. Of cloud security and future threats, the NCSC report said (on page 26):

> "Only 40% of all data stored in the cloud is access secured, although the majority of companies report they are concerned about encryption and security of data in the cloud. As more organisations decide to move data to the cloud (including confidential or sensitive information) it will become a tempting target for a range of cyber criminals. They will take advantage of the fact that many businesses put too much faith in the cloud providers and don't stipulate how and where their data is stored."

However, the NCSC recognises that from a security perspective, using a public cloud service where the CSP has made the 'right security investments' may offer several advantages, including configuration, the CSP's security bench depth, strength of security patches and focused alerts.[11]

[7] Threats include (i) botnets (computer networks remotely and maliciously controlled), (ii) DDoS (distributed denial of service) attacks, (iii) hacking (unauthorised system access), (iv) malware (malicious software), (v) phishing (unauthorised access to a person's identity), (vi) ransomware (disabling malware unlocked on payment), (vii) spam (unsolicited communications), (viii) spyware (surveillance malware), (ix) trojan horses, (x) viruses and (xi) worms (as self-replicating malware enabling unauthorised access).

[8] The National Cyber Security Centre, part of GCHQ (the UK Government's Communications Headquarters), 'acts as a bridge between industry and government, providing a unified source of advice, guidance and support on cyber security, including the management of cyber security incidents' (https://www.gov.uk/government/organisations/national-cyber-security-centre).

[9] '*The cyber threat to UK business 2017-2018 report*', 10 April 2018 - https://www.ncsc.gov.uk/cyberthreat

[10] GDPR Art 4(12) defines a 'personal data breach' as 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'.

[11] '*Brightening the outlook for security in the cloud*', NCSC, 26 September 2017, https://www.ncsc.gov.uk/blog-post/brightening-outlook-security-cloud

7. **Cloud benefits therefore need to be balanced against security concerns**. For enterprise users, the cloud provides a range of benefits and opportunities, including provisioning flexibility, access to new services, assisting digital transformation, speed of deployment and cost efficiencies. However, enterprise-scale organisations operate in a business environment that increasingly emphasises the criticality of cloud and data security - the legal, technical, operational and governance controls put in place to ensure desired information security outcomes. Research consultancy IDC in their 'Data Age 2025' White Paper (see footnote 1 above) calls out (at page 3) security as one of five key trends that will intensify the role of data and the cloud:

> "All this data from new sources open up new vulnerabilities to private and sensitive information. There is a significant gap between the amount of data being produced today that requires security and the amount of data that is actually being secured, and this gap will widen — a reality of our data-driven world. By 2025, almost 90% of all data created in the global datasphere will require some level of security, but less than half will be secured."

As IT workloads migrate to the cloud, the benefits of cloud provisioning therefore need to be weighed, balanced and managed against security risks and duties. Even as the debate shifts to a general perception that the cloud is more secure than on-prem, the huge current and forecast growth means that cloud security remains the central preoccupation both of CSPs and their customers.

8. **Reprise: cloud terminology**. The classic definition[12] of the cloud specifies a type of computing with five characteristics, three service models and four deployment models.

a) ***cloud characteristics***: the key characteristics are:

- ***on-demand self-service***: the customer can obtain computing resources automatically as needed without CSP intervention;
- ***broad network access***: computing resources can be accessed through standard mechanisms anytime, anywhere;
- ***resource pooling***: the CSP's computing resources are pooled serving multiple customers on a multi-tenant basis;
- ***rapid elasticity***: computing resources can be quickly scaled as needed so the customer can respond to business demand without taking capacity resourcing risks; and
- ***measured service***: consumption can be monitored and controlled and the customer pays for the resources it uses.

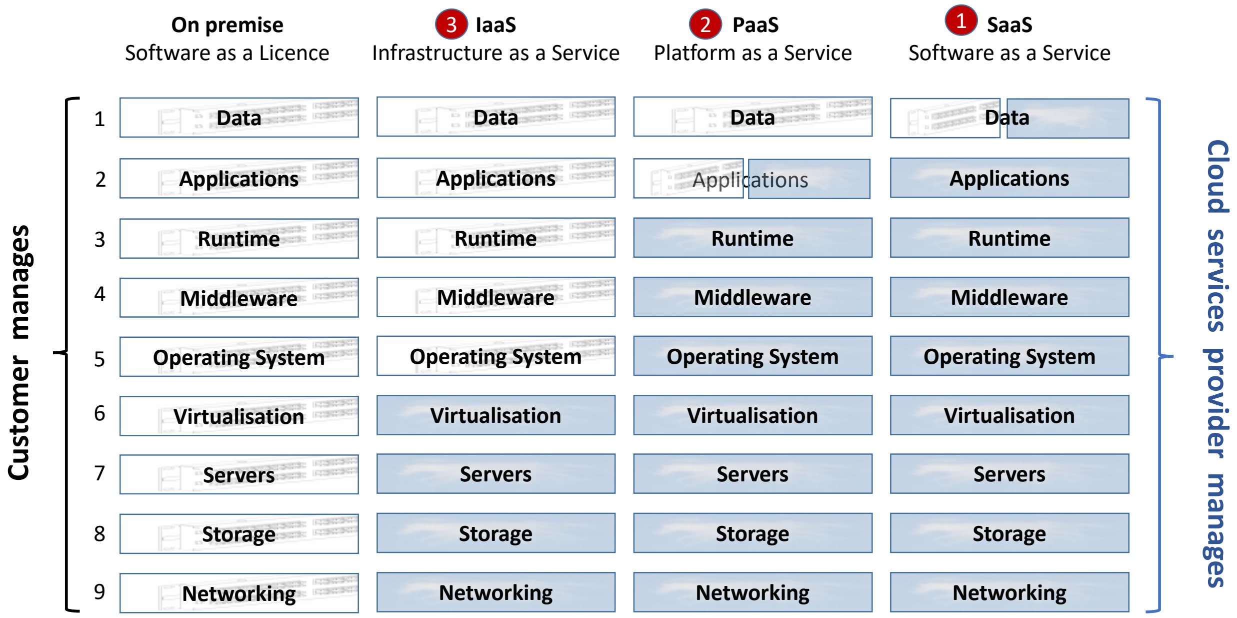
b) ***cloud service models***. The three traditional service models of cloud computing are ***Software as a Service*** (***SaaS***), ***Platform as a Service*** (***PaaS***) and ***Infrastructure as a Service*** (***IaaS***). Their constituent parts in the computing stack and the distinctions between them are shown at 1, 2 and 3 in Figure 2 below. As the cloud develops and new services proliferate, it is now common to speak of ***Anything as a Service*** (***XaaS***).

[12] available on the NIST (US National Institute of Standards and Technology) website at http://www.nist.gov/itl/cloud/

c) ***cloud deployment models***. The four main deployment models of cloud services are:

- ***private cloud***: where infrastructure, platform or software are dedicated to one customer;
- ***public cloud***: where service is provided to customers on a multi-tenant basis;
- ***hybrid cloud***: as private cloud with access to public cloud to manage peaks; and
- ***community cloud***: used by a community of customers rather than a single one.

Figure 2: Software 'as a Licence' to Software 'as a Service': Cloud Service Model Continuum



	On premise Software as a Licence	3 IaaS Infrastructure as a Service	2 PaaS Platform as a Service	1 SaaS Software as a Service
1	Data	Data	Data	Data
2	Applications	Applications	Applications	Applications
3	Runtime	Runtime	Runtime	Runtime
4	Middleware	Middleware	Middleware	Middleware
5	Operating System	Operating System	Operating System	Operating System
6	Virtualisation	Virtualisation	Virtualisation	Virtualisation
7	Servers	Servers	Servers	Servers
8	Storage	Storage	Storage	Storage
9	Networking	Networking	Networking	Networking

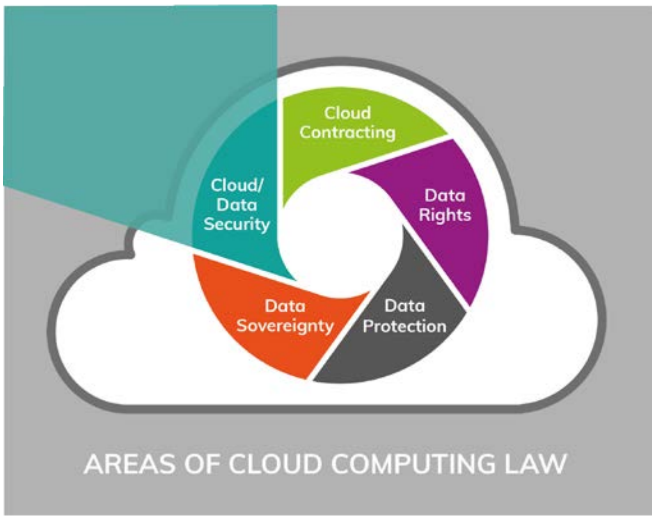
d) ***'core'**, **'edge'** and **'containers'***: as the cloud develops, it is becoming increasingly common to speak of its 'core' and 'edge', and 'containers':

- the ***'core'*** is the cloud's engine room - the 500 or so hyperscale, and all the other, data centres around the world that make up the cloud;
- the ***'edge'*** is where the cloud connects with the billions of IoT sensors and other devices at the edge of the physical world. Tuned by machine learning baked into the software that runs cloud operations and hunts for cost efficiencies, edge computing enables data generated by IoT and other devices to be processed close to source and away from the core;[13]
- '***containers***' are small, discrete, independently deployable applications designed to run anywhere that carry the bare minimum resources to do a specific job. Containers boost the cloud's efficiency by enabling routine processing tasks to be carried out on the edge where the data is generated, avoiding the unnecessary journey to the core and back again. More technically, containers are to OS (operating system) virtualisation what the hypervisor is to machine virtualisation. Unlike a VM (virtual machine), containers do not contain an operating system but call on OS resources via an API (application programming interface).

[13] See '*the future of computing is at the edge*', Richard Waters, Financial Times, 6 June 2018 - https://www.ft.com/content/1dba534a-5857-11e8-bdb7-f6677d2e1ce8

9. **Areas of cloud computing law**. Security is one of a number of rapidly developing areas of cloud computing law. These areas overlap to an extent and may best be thought of as providing different perspectives and frameworks from which to analyse and assess cloud computing law issues. They may very briefly be summarized as follows:

- ***cloud/data security***: the legal, technical, operational and governance controls that an organisation puts in place to ensure desired cloud data security outcomes;
- ***cloud contracting***: the cloud service agreement between CSP and its customer;
- ***data rights***: the intellectual property and other rights that arise in relation to data;
- ***data protection***: the legal rights and duties that arise in relation to personal data;
- ***data sovereignty***: the right of a person to control access to their data by a third party (generally a state agency).



This white paper focuses on cloud security. It is distinguished from data protection as covering not only personal and but all other data of the enterprise; from data security generally as covering data in (or in transit to or from) the cloud rather than on premises, on the device or elsewhere; and from data sovereignty as being limited to the cloud (but there covering more than third party powers to intercept or access communications data). Rights will typically arise in relation to data irrespective of the types of data concerned or where the processing giving rise to those rights takes place. For our resources on these other legal aspects of cloud computing, please see our white papers and blogs on cloud contracting,[14] data rights,[15] data protection[16] and data sovereignty[17].

10. **Aims and scope of this white paper**. This paper is designed to overview relevant issues and to set out primarily by way of checklists the sources of cloud security legal duties relating to the enterprise (**Section B**) and the practical steps that enterprises may take in order to mitigate cloud security risks (**Section C**). This paper is written as at 31 May 2018 and from the perspective of English law, making reference to other countries' laws where relevant.

[14] http://www.kempitlaw.com/law-firms-and-contracting-for-the-cloud/

[15] http://www.kempitlaw.com//wp-content/uploads/2014/10/Legal-Aspects-of-Big-Data-White-Paper-v2-1-October-2014.pdf

[16] http://www.kempitlaw.com//wp-content/uploads/2014/10/Big-Data-and-Data-Protection-White-Paper-v1_0-November-2014.pdf

[17] http://www.kempitlaw.com/cloud-computing-and-data-sovereignty/

B. SOURCES OF ENTERPRISE CLOUD SECURITY DUTIES

11. **Checklist of sources of enterprise-related cloud security duties**. As enterprise computing workloads move to the cloud, the benefits of cloud provisioning need to be weighed and balanced against security legal risks and obligations. Organisations are therefore establishing cloud security and compliance frameworks and governance to manage the range of cloud security duties and to assess, advise on and assist in managing the risks that are involved.

The start point here is a checklist of the sources of cloud security duties that may apply to the enterprise. These obligations are diverse and increasingly far reaching, and will vary by industry sector. The enterprise in the cloud will need to consider not only its own regulatory duties but also those of its customers and supply chains, as well as other generally applicable information security obligations. Enterprises will also need to consider multiple (and potentially conflicting) cloud security obligations across their international operations. To assist in the process, we have provided the following checklist of the sources of enterprise-related cloud security duties.

Table 1: Checklist of Sources of Enterprise-Related Cloud Security Duties and Liabilities

A.	**ENTERPRISE - REGULATORY DUTIES**
1.	**Sector specific regulation**
a)	Example 1: UK financial services firms regulated by the Financial Conduct Authority (FCA)
	• European Banking Authority March 2018 (EBA/REC 2017/03): Cloud Outsourcing Recommendations[18] • FCA July 2016 (FG16/5): Guidance for enterprises outsourcing to the 'cloud' and other third party IT services[19] • FCA Handbook SYSC Rule 8 (General outsourcing risk management controls)[20] and DTR (Disclosure and Transparency Rules)[21] • Directive 2009/138/EC (Solvency II) for insurers: Articles 38 and 49 (outsourcing)[22]
b)	Example 2: UK law firms authorised by Solicitors Regulation Authority (SRA)
	• SRA high-level Principles[23] • SRA Code of Conduct[24] - Outcome 7.10: outsourcing requirements (applies to cloud services)

[18] https://www.eba.europa.eu/documents/10180/2170125/Recommendations+on+Cloud+Outsourcing+%28EBA-Rec-2017-03%29_EN.pdf/e02bef01-3e00-4d81-b549-4981a8fb2f1e

[19] UK Financial Conduct Authority - https://www.fca.org.uk/publications/finalised-guidance/fg16-5-guidance-firms-outsourcing-%E2%80%98cloud%E2%80%99-and-other-third-party-it

[20] FCA's Senior Management Arrangements, Systems and Controls (SYSC) - https://www.handbook.fca.org.uk/handbook/SYSC/8/

[21] https://www.handbook.fca.org.uk/handbook/DTR/

[22] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32009L0138&from=EN

[23] https://www.sra.org.uk/solicitors/handbook/handbookprinciples/content.page

[24] https://www.sra.org.uk/solicitors/handbook/code/content.page

2.	**Generally applicable security/data regulation**
a)	Data protection/privacy – GDPR (Regulation 2016/679):[25] enterprise as data controller
	• controller must comply with Art. 5 personal data processing principles, including 'ensuring appropriate security … using appropriate technical or organisational measures' (Art 5(1)(f)) • controller 'shall implement appropriate technical and organisational measures to ensure and be able to demonstrate that processing is performed in accordance with' GDPR (Art 24(1)) • controller must 'implement appropriate technical and organisational measures designed to implement data-protection principles' (Art 25(1)) • controller 'shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures' so that processing complies with the GDPR (Art 28(1))
b)	Security of network and information systems (duties applicable to CSPs)
	NIS Directive 2016/1148 and UK implementing regulations, SI 2018/506[26]
	• a CSP 'must identify and take appropriate and proportionate measures to manage the risks posed to the security of network and information systems on which it relies to provide its service' (Reg 12(1) implementing Directive, Art 16(1))[27] • those measures must 'prevent and minimise the impact of incidents … and take into account (i) the security of systems and facilities, (ii) incident handling, (iii) business continuity management, (iv) monitoring auditing and testing and (v) compliance with international standards' (Reg 12(2), implementing Art 16(1))
	Communications Act 2003[28] (CA 2003) Privacy and E-Communications Regulations 2003[29] (PECR)
	• notification requirements/notifications in relation to a breach of or failure to take appropriate organisational and technical measures, etc: o by a CSP as a public electronic communication network (PECN) under S.105(A) CA 2003 or in relation to a security breach under S.105B CA 2003; o by a CSP as a public electronic communications service (PECS) provider under Reg 5 PECR;

[25] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN. GDPR came into force on 25 May 2018. The UK Data Protection Act 2018 also came into force on this date - http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf.

[26] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN. The NIS Regulations (SI 2018/506) - https://www.legislation.gov.uk/uksi/2018/506/made - implemented the NIS Directive into English law on 10 May 2018.

[27] The Directive and UK Regulations apply to relevant 'digital services providers' and the 'operators of essential services'. 'Cloud computing services', as 'enabling access to a scalable and elastic pool of shareable computing resources' are 'digital services' regulated by Articles 16-18 of the Directive and Regulations 12-14 of the UK SI.

[28] https://www.legislation.gov.uk/ukpga/2003/21/contents

[29] http://www.legislation.gov.uk/uksi/2003/2426/contents/made. Note: as at end May 2018, discussions are still under way at EU level to replace the ePrivacy Directive (2002/58) - https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002L0058&from=EN - with a directly applicable ePrivacy Regulation.

c)	Data sovereignty – Investigatory Powers Act 2016[30]
	• regulates powers for interception and to retain and access communications data • interception - interfering with or monitoring a communication in course of transmission by which its content (message + envelope) is seen otherwise than by sender or recipient[31] • communications data - ‘the ‘who’, ‘when’, ‘where’ and ‘how’ of a communication, but not the content, not what was said or written’[32]
d)	Data residency/domiciliation and related requirements
	• EU: unauthorised international transfers of personal data are unlawful (GDPR, Art 44) • Countries (including Russia, China and Vietnam) with data domiciliation laws
e)	UK criminal law
	Official Secrets Act 1989
	• Crown servants and UK government contractors disclosing of or failing to secure information damaging to the UK’s interests may commit offences
	Computer Misuse Act 1990
	• hacking (as unauthorised access) and DDOS (distributed denial of service attacks) and various cyber activities can be offences
	UK Terrorism Acts 2000-2015
	• introduces terrorism offences in relation to cyber security
	UK Fraud Act 2006
	• phishing/identity theft (dishonestly and knowingly making a false representation intending gain or loss) can be an offence
3.	**Relevant generally applicable business regulation**
	• public companies’ governance requirements under the Companies Act 2006 (CA 2006) • company law duties under CA 2006 to retain accounting/general records • directors’ CA 2006 duty to exercise reasonable skill, care and diligence • litigation procedure duties relating to document discovery
B.	**ENTERPRISE – (NON-CONTRACTUAL) CIVIL LAW DUTIES**
4.	**Negligence: towards a general duty of care in tort?**
	• the general duty to take “appropriate technical and organisational measures” to keep data secure in the cloud is emerging as the cybersecurity yardstick by which the normal tortious/negligence duty to “take reasonable care” looks likely to be measured.
5.	**A cloud security incident may give rise to other civil liability including:**
	• breach of confidence, copyright (other intellectual property), fiduciary or statutory duty • misuse of private information, conversion, negligence (see above), trespass

[30] http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted

[31] Investigatory Powers Act 2016, section 4

[32] UK Home Office, ‘*Acquisition and Disclosure of Communications Data*’ Code of Practice, March 2015, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/426248/Acquisition_and_Disclosure_of_Communications_Data_Code_of_Practice_March_2015.pdf

C.	**ENTERPRISE – CONTRACTUAL DUTIES**
6.	**Contractual – between Enterprise and its Customers**
a)	agree customers' general/specific data security regulatory requirements
	• customer vendor policies: (i) data security, (ii) physical/logical security, (iii) data retention, (iv) disaster recovery/business continuity, (v) business conduct, (vi) audit, (vi) vendor supply-chain flowdown • agree on scope of 'appropriate technical and organizational measures' if relevant • data sovereignty/residency-domiciliation requirements
b)	GDPR
	• cover off enterprise's GDPR obligations as controller/processor of customers' information • as controller – GDPR compliant data sharing • as processor – GDPR Art. 28(3) duties, subprocessors/ supply chain/ international transfers, etc
c)	'normal', market standard data access, ownership/licensing, return terms
7.	**Contractual - between Enterprise and its Suppliers**
a)	For Enterprise as customer, see inverse of C.6 a)-c) (particularly for IT vendors to Enterprise)
b)	specific requirements of particular suppliers – e.g. Enterprise's insurers and record retention
8.	**Contractual – between Enterprise and CSP**
a)	Security Assessment
	• Hosting: (i) where is data hosted? (ii) who is the data centre provider? (iii) what is the type of hosting (shared/dedicated virtual/physical server, private cloud, etc) • Encryption: (i) what encryption is in place, (ii) who manages the encryption keys? • Managing: (i) releases, (ii) access, (iii) support, (iv) data retention, (v) continuity, (vi) incidents
b)	What certifications and assessments does the CSP have in place to assure compliance?
	e.g. (i) ISO/IEC 27001 (information security management), (ii) ISO/IEC 27108 (personal data in the public cloud), (iii) ISO/ IEC 38500 (IT Governance), (iv) ISO/IEC 38505 (data governance), (v) SSAE 16/18 SOC II, etc
D.	**ENTERPRISE – INTERNAL POLICIES/PROCEDURES**
	• IT/acceptable use policies – to cover cloud use • Website/employee privacy policies • Range of GDPR policies, procedures, documentation to demonstrate GDPR compliance • Training and awareness • Employee/consultant duties of confidentiality, etc • Device controls (particularly for BYOD (Bring Your Own Device) • Password controls/policies • Vulnerability assessment/penetration testing, etc

C. TOWARDS CLOUD SECURITY BEST PRACTICES

12. **A three step approach: (i) data classification, (ii) cloud security best practices, (iii) assurance**. In this section, we are suggesting a 3-step approach to best practice built around:

(i) data classification (***paragraphs C.13** to **C.17***),

(ii) cloud security best practices, principles and commitments applicable for the data so classified (***paragraphs C.18** and **C.19***); and

(iii) obtaining assurance from the CSP on its cloud security commitments (***paragraphs C.20** and **C.21***).

We provide at Table 2 checklist for cloud best practices. This is drawn in part from the suite of cloud security documents that the NCSC and other parts of the UK Government ('HMG') have prepared. We have collated and provided links to them in the Annex to this paper.

13. **(i) Data classification - general** . A structured approach to data classification is a critical tool for managing an organisation's data assets. Data subsists in one of three states (at rest, in process, in transit), can be either structured or unstructured and is subject to access control based on authentication (verifying that the user is who they say they are) and authorisation (providing an authenticated user with the ability to access the data concerned). A particular data classification requires a terminology model articulating levels of classification sensitivity. It will also take into consideration:

- the nature of the data (personal, confidential, highly sensitive, publicly available, acquired under third party licence, proprietary to the organisation, etc);
- its source, purposes and use cases; data compliance considerations (like the jurisdictions of origin and domicile of the data); and
- other relevant business, contractual and legal constraints.

In the words of a 2014 Microsoft white paper, *Data Classification for Cloud Readiness*:[33]

> "Data classification provides one of the most basic ways for organizations to determine and assign relative values to the data they possess. The process of data classification allows organizations to categorize their stored data by sensitivity and business impact in order to determine the risks associated with the data. After the process is completed, organizations can manage their data in ways that reflect its value to them instead of treating all data the same way. Data classification is a conscious, thoughtful approach that enables organizations to realize optimizations that might not be possible when all data is assigned the same value."

14. **(i) Data classification – HMG's 2013 review**. Driven in large part by the digitisation of UK public sector workloads, HMG in 2013 carried out a major overhaul of the way in which it classified the UK's data assets. This led to the Government Security Classifications guidance published in April 2014 (Annex, point 3.1) when the longstanding five level classification that then applied[34] was replaced with a new three level system of OFFICIAL→SECRET→TOP SECRET.

[33] https://www.microsoft.com/en-us/search/result.aspx?q=data+classification+for+cloud+readiness

[34] UNCLASSIFIED → RESTRICTED → CONFIDENTIAL → SECRET → TOP SECRET

At a time when the cloud's share of enterprise IT is set to rise from 10% to 45% within the next decade, HMG's approach to data security classification has important lessons for the enterprise in differentiating between data classes and the security controls and hence cloud service costs that apply to them.

15. **(i) Data classification - HMG data at OFFICIAL**. The reduction from five to three classes was critical in respect of the new OFFICIAL category, where, in the 'key points' section of its briefing to suppliers (Annex, point 3.2), the Cabinet Office said:

> "The OFFICIAL classification covers up to *ninety percent of Public Sector business*, including most policy development, service delivery, legal advice, personal data, contracts, statistics, case files, and administrative data.
>
> - Security controls at OFFICIAL are based on good, commercially available products, in the same way that the best-run businesses manage their sensitive information.
> - Particularly sensitive OFFICIAL information will be controlled through local handling arrangements that reinforce the 'need to know' principle (emphasis added)."

Page 7 of the UK Government Security Classifications guidance highlights examples of what is considered OFFICIAL, including:

> "• The day to day business of government, service delivery and public finances.
> - Routine international relations and diplomatic activities.
> - Public safety, criminal justice and enforcement activities.
> - Many aspects of defence, security and resilience.
> - Commercial interests, including information provided in confidence and intellectual property.

Personal information that is required to be protected under the Data Protection Act (1998) or other legislation (e.g. health records)."

16. **(i) Data classification – associating security controls to particular classes of data**. A data classification framework is not only about placing data in the appropriate sensitivity category, but also about associating the right level of security controls with that data. The UK approach dictates that OFFICIAL information:

> "must be secured against a threat model that is broadly similar to that faced by a large UK private company"[35]

with levels of security controls that:

> "are based on good, commercially available products in the same way that the best-run businesses manage their sensitive information"[36]

so that consequently:

> "this change in approach will enable the public sector to take advantage of a wider range of modern, lower cost (commodity) security products rather than defaulting to expensive, bespoke or augmented technologies."[37]

[35] '*Government Security Classifications'* (April 2014) at Annex, point 3.1, page 18 below

[36] '*Government Security Classifications Supplier Briefing'* (October 2013) at Annex, point 3.2

[37] Page 5, FAQ 2 – '*Managing Information Risk at OFFICIAL*' at Annex, point 3.5

17. **(i) Data classification - benefits outweigh costs as cloud share of enterprise IT rises?** As the migration of enterprise computing workloads to the cloud gathers pace, the costs savings and other benefits involved in more closely calibrating cloud security controls to particular classes of data – and avoiding the excess costs inherent in classifying all data the same – will increasingly outweigh the burden of the administrative effort and expense in putting in place the necessary systems and procedures.

18. **(ii) Cloud security best practices – a range of approaches.** Many organisations now document cloud security best practices. In the private sector, good examples include the CSP- (supplier-) side approaches from AWS (AWS Security Best Practices, August 2016), Cloud Security Alliance (CSA Security Guidance 4.0, February 2018) and Microsoft (Microsoft Cloud Security for Enterprise Architects, August 2017). Governments and public sector organisations have tended to take the lead on cloud security best practice from the customer side. At EU level, ENISA (the EU Agency for Network and Information Security) in February 2015 in its report *Security Framework for Governmental Clouds*[38] proposed a security framework modelled on four 'Plan → Do → Check → Act' lifecycle phases summarised in table 2.

Table 2: Best Practices - ENISA Security 'Plan-Do-Check-Act' Lifecycle Framework

	Security Activity	Security Step
PLAN	a) Risk profiling	1. Identify services to cloudify 2. Select security dimensions[39] 3. Evaluate individual impact to these dimensions 4. Determine global risk profile
	b) Architectural model	5. Decide on deployment – service model[40]
	c) Security/privacy requirements	6. Establish security requirements
DO	d) Security controls	7. Selection of security controls
	e) Implementation deployment & accreditation	8. Formalisation and implementation of selected security controls 9. Cloud service suitability ex ante verification to provide sufficient assurance 10. Start service execution
CHECK	f) Log/monitoring	11. Periodically check that security controls are in place and being followed
	g) Audit	12. Verification that the defined/contracted levels of security are fulfilled
ACT	h) Change management	13. Implementation of remedies & improvement to security framework/approach
	i) Exit management	14. Contract termination, return of data to customer and data deletion

[38] Available at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/governmental-cloud-security/security-framework-for-govenmental-clouds

[39] Based on availability, integrity and confidentiality

[40] Whether public, private, hybrid or community, cloud

19. **(ii) Cloud security best practices – NCSC’s cloud security principles**. In the UK the NCSC published in September 2016 fourteen principles for cloud security and has also, along with other HMG departments, produced the suite of cloud security documents referred to in the Annex to this White Paper. Although naturally geared to the public sector, the NCSC approach lends itself to use in the enterprise, and for our checklist of cloud security best practices at Table 3, we have adopted the NCSC’s approach as a basis to work from. This is because (i) its approach is from the cloud user’s, not the CSP’s, perspective and so more in line with the position of the enterprise; (ii) the NCSC approach is comprehensive, transparent and accessible; and (iii) HMG/NCSC have done much of the heavy lifting. We include in the checklist the fourteen Cloud Security Principles. The full (25 page) HMG ‘*Implementing the Cloud Security Principles*’ document is available via the link at point 4.4 of the Annex. The full document drills down to much useful detail at the level below the principles themselves, setting out for each principle the aspects to be considered, goals, implementation approaches and additional notes.

Table 3: Checklist of Best Practices for Enterprise Cloud Security

(i)	**DATA CLASSIFICATION**
	See paragraphs C.13 to C.17 above.
(ii)	**CLOUD BEST PRACTICES: THE NCSC’S 14 CLOUD SECURITY PRINCIPLES**[41]
	Cloud Security Principle /Checklist Question
	1. Data in transit protection Is Enterprise data transiting networks adequately protected against tampering and eavesdropping by the CSP?
	2. Asset protection and resilience Is Enterprise data, and the assets storing or processing it, protected against physical tampering, loss, damage or seizure by the CSP?
	3. Separation between consumers Will a malicious or compromised service user be able to affect the service or data of another user?
	4. Governance framework Does the CSP have a security governance framework which coordinates and directs its management of the service and information within it. Are any technical controls deployed outside of this framework?
	5. Operational security Does the CSP operate/manage the service securely in order to impede detect or prevent attacks? (Good operational security should not require complex, bureaucratic, time consuming or expensive processes).

[41] Headline points. See the NCSC’s full document at Implementing the Cloud Security Principles

	6. Personnel security Does the CSP screen/adequately train its staff? (Where service provider personnel have access to your data and systems you need a high degree of confidence in their trustworthiness. Thorough screening, supported by adequate training, reduces the likelihood of accidental or malicious compromise by service provider personnel.)
	7. Secure development Is the CSP's service designed and developed to identify and mitigate threats to its security? (Those which aren't may be vulnerable to security issues which could compromise the Enterprise's data, cause loss of service or enable other malicious activity.)
	8. Supply chain security Does the CSP ensure that its supply chain satisfactorily supports all of the security principles which the service claims to implement?
	9. Secure consumer management Does the CSP make the tools available for secure management of the Enterprise's use of the CSP's service? (Management interfaces and procedures are a vital part of the security barrier, preventing unauthorised access and alteration of Enterprise resources, applications and data).
	10. Identity and authentication Is all access to service interfaces constrained to authenticated and authorised individuals?
	11. External interface protection Are all external or less trusted interfaces of the service identified and appropriately defended?
	12. Secure service administration Do all administration systems for the CSP's service have highly privileged access to that service? (Their compromise has significant impact, including the means to bypass security controls and steal or manipulate large volumes of data.)
	13. Audit information provision to consumers Does the CSP undertake to provide the Enterprise with the audit records it needs to monitor access to the service and the data held within it? (The type of audit information available to the Enterprise will have a direct impact on its ability to detect and respond to inappropriate or malicious activity within reasonable timescales).
	14. Secure use of the service by the Enterprise The security of the CSP's service and the data held within it can be undermined if the Enterprise uses the service poorly. Does the Enterprise have to undertake reasonable, specific (so measurable) responsibilities when using the service in order for the Enterprise's data to be adequately protected?

(iii)	OBTAINING ASSURANCE FROM THE CSP ON ITS CLOUD SECURITY COMMITMENTS
	The NCSC document having confidence in cyber security explains the ways in which cloud buyers can determine and demonstrate compliance with the principles. These include: • CSP assertion • CSP contractual commitment • third party certification • independent testing • a mix of one or more of these.
	How does the CSP propose to give the Enterprise satisfactory assurance that it will comply with its cloud security commitments?
	Does the CSP have ISO 27001[42] (on information security management systems) certification?
	Does the CSP have SSAE 16/18, Soc 2 [Type II][43] certification?
	Questions: (a) Has the certification been issued by an approved certifier? (b) Is the certification accompanied by the full, relevant report and all other necessary supporting documentation? (c) Is the certification still current? (d) Does the certification cover the CSP service that is to be contracted for? (e) Does the certification cover all data centres/locations at which Enterprise data will be stored? (f) Will the CSP undertake to keep all certifications in force for the duration of the agreement, including by renewing any that time out or lapse? (g) If the CSP loses any relevant committed certification, is the CSP required to notify the Enterprise promptly? (h) Can the Enterprise terminate for CSP breach in these circumstances?

20. **(iii) Obtaining assurance from the CSP on its cloud security commitments**. Section III of the checklist at Table 3 addresses the third step of the suggested approach to cloud security – how the CSP can provide assurance that it will meet its security commitments. The NCSC paper having confidence in cyber security explains the ways in which cloud buyers can determine and demonstrate compliance with the cloud security principles. These include (i) CSP assertion, (ii) CSP contractual commitment, (iii) third party certification, (iv) independent testing or (v) a mix of one or more of these.

In our experience, of all the ways in which cloud users can obtain assurance from the CSP that it will meet its cloud security commitments, the combination of [contractual commitment] + [accredited standards certification] + [reserving the right to carry out independent testing] is emerging as standard market practice.

[42] See http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

[43] https://www.ssae-16.com/ Note that SSAE 18, effective as of 1 May 2017, superseded SSAE 16 (and its predecessor, SAS 70)

21. **(iii) Obtaining assurance – standards**. The most commonly invoked security standards in cloud contracting at the moment are ISO/IEC 27001 (information security management systems) and SSAE 18, SOC 2 reporting (which evaluates an organisation's information systems relevant to security, availability, processing, integrity, confidentiality or privacy). The checklist above raises a number of questions for each that will be relevant in the contracting context. A range of further ISO/IEC standards are now being used or under development to confer assurance on data governance and use, and many will be relevant to cloud services, including the following:

- ***Data governance***
    - ISO/IEC 38500 on ICT governance for the organization;
    - ISO/IEC 38505-1, applying ISO/IEC 38500 specifically to governance of data;
    - ISO/IEC 38507 – governance implications of Artificial Intelligence;
- ***Relevant to use of data in cloud services***:
    - ISO/IEC 29100 on a privacy framework for ICT security techniques;
    - ISO/IEC 27018 on the protection of personally identifiable information in the pubic cloud;
    - ISO/IEC 19944, addressing data categories, flows and use for cloud services and devices;
    - ISO/IEC 27552 on extending ISO/IEC 27001 and ISO/IEC 27002 to privacy information management (under development); and

ISO/IEC 23053, framework for Artificial Intelligence using Machine Learning (under development).

22. **Conclusion**. Enterprise cloud migration is set to gather pace in the coming months and years, bringing a wide range of IT benefits to large organisations. As we have seen recently with GDPR, security is in the public eye, and legal duties to keep cloud data secure are becoming more onerous. Balancing cloud benefits and security duties is therefore a critical success factor for organisations in their cloud operations. Ensuring cloud security - the mix of legal, technical, operational and governance measures to achieve a desired information security outcome – is moving centre stage as enterprises shift their computing workloads 'off prem'. Putting in place effective cloud security governance frameworks, and the policies, procedures and processes that underpin them, will become indispensable. This White Paper aims to assist the process by providing checklists of security responsibilities and best practices to address them.

Richard Kemp,
Kemp IT Law, London,
June 2018
richard.kemp@kempitlaw.com

ANNEX: HMG SECURITY, DATA CLASSIFICATION AND CLOUD SECURITY POLICY GUIDANCE[44]

No.	Title	Date	URL	Status (05.2018)
1.	**ICT STRATEGY**			
1.1	Government Transformation Strategy	February 2017	https://www.gov.uk/government/publications/government-transformation-strategy-2017-to-2020/government-transformation-strategy	In effect
1.2	Government ICT Strategy: Strategic Implementation Plan[3]	October 2011	https://www.gov.uk/government/publications/government-ict-strategy-strategic-implementation-plan	Superseded by 1.4
1.3	Government Cloud Strategy	October 2011	https://www.gov.uk/government/publications/government-cloud-strategy	Not withdrawn
1.4	Government Service Design Manual	June 2015	https://www.gov.uk/service-manual	In effect
1.5	Digital by Default Service Standard	June 2015	https://www.gov.uk/service-manual/service-standard	In effect
2.	**SECURITY POLICY**			
2.1	Government Security Policy Framework	v1.1 May 2018	https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework	In effect
3.	**SECURITY AND DATA CLASSIFICATION**			
3.1	Government Security Classifications	Updated May 2018	https://www.gov.uk/government/publications/government-security-classifications	In effect
3.2	Government Security Classifications Supplier Briefing	October 2013	https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/251481/Government-Security-Classifications-Supplier-Briefing-Oct-2013.pdf	Current

[44] The UK Government documents listed here are Crown Copyright and (mainly) licensed under the terms of the Open Government Licence (available at https://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/). The licence permits worldwide use and copying, publication, distribution, transmission and adaptation of content and commercial and non-commercial exploitation subject to acknowledgement and a default attribution of 'Contains public sector information licensed under the Open Government Licence v3.0'.

No.	Title	Date	URL	Status (05.2018)
3.3	Government Security Classifications – Supplier Slides	October 2013	https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/251482/Government-Security-Classifications-Supplier-Slides-Oct_2013.pdf	Current
3.4	FAQ 1 - Working With Official Information	April 2013	https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/709004/May-2018_Working-with-OFFICIAL.PDF	Current
3.5	FAQ 2 – Managing Information Risk at OFFICIAL	V2.0 March 2014	https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/286667/FAQ2_-_Managing_Information_Risk_at_OFFICIAL_v2_-_March_2014.pdf	Current
4.	**CLOUD SECURITY**			
4.1	Introduction: Understanding Cloud Security	August 2016	https://www.ncsc.gov.uk/guidance/introduction-understanding-cloud-security	In effect
4.2	Having Confidence in Cyber Security	August 2016	https://www.ncsc.gov.uk/guidance/how-confident-can-you-be-cloud-security	In effect
4.3	Introduction to Risk Management for Cyber Security Guidance	December 2017	https://www.ncsc.gov.uk/guidance/introduction-risk-management-cyber-security-guidance	In effect
4.4	Implementing the Cloud Security Principles	Sept 2016	https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles	In effect
4.5	Separation and Cloud Security	August 2016	https://www.ncsc.gov.uk/guidance/separation-and-cloud-security	In effect
4.6	IaaS – Managing Your Responsibilities	August 2016	https://www.ncsc.gov.uk/guidance/iaas-managing-your-responsibilities	In effect
4.7	Cloud Security Guidance: Standards and Definitions	August 2014	https://www.gov.uk/government/publications/cloud-security-guidance-standards-and-definitions	In effect