UCD IT Services

Security Assurance review for Microsoft Cloud Service adoption at UCD

CONTENTS

Version Control

Version	Notes	By
0.2	Initial for internal review	J. Curran
1.0	Approved for issue	John Curran

INTRODUCTION

IT Services in UCD has adopted the Microsoft Online Services "Office 365" platform for use within the UCD community, initially as a pilot deployment of personal storage and document management "OneDrive", personal collaboration and messaging "Lync", and group document collaboration "Sharepoint Online". IT Services are currently planning deployment of the platform for staff and students, meaning that personal and group collaboration, storage and communication will be hosted and accessible from Microsoft.

At present, UCD owns or manages personal information and data pertaining to almost a quarter of a million people, and operational systems such as UCD Connect are used by upwards of 30,000 people on a daily basis. Assuming, for the purposes of conducting a due diligence assessment, that UCD's stored files and group materials will move entirely to Microsoft as a long term goal, this means that, other than email, Microsoft will host the majority of UCD's operational documents, document based records and data over time.

Planning to migrate UCD data raises data governance and security issues in the areas of access security, data protection, custodianship and ownership.

In addition, the emergence of globally managed cloud based services has also presented legal challenges from a data protection regulatory perspective. Legislation and mechanisms in place to enforce data protection currently derive in origin from the 1988 Data Protection act and as amended, and the replacement regulatory framework, currently at EU Commission proposal stage from the Article 29 working group, is not expected to come into force until at least 2015[1].

This document aims to review the issues involved and considers the following issues:

1. What are the security risks presented by migration to Microsoft?
2. Are the security risks presented by the use of Microsoft's cloud well managed from a UCD perspective?
3. Are there any immediate regulatory barriers to the use of Microsoft cloud services for UCD's documents or other cloud hosted services?
4. Are there any regulatory\legal issues impacting Microsoft that impinge on UCD's data security?
5. Does UCD have viable future exit strategies?

SUMMARY, KEY FINDINGS AND RECOMMENDATIONS

KEY FINDINGS:

Finding 1: Microsoft's baseline service offerings present demonstrable independent assurance of risk management and security equivalence at a minimum to UCD's current security environment. Microsoft services have independent security reviews conducted to industry standards, and retain these certifications under SSAE 16 SOC1 Type II, ISO 27001, and HIPAA. Summary copies of the most recent available versions of these have been reviewed by UCD IT Services. In April this year, a working group of Data protection authorities across Europe approved Microsoft's EU Data Protection compliance framework[2].

[1] See Data Protection references

[2] See Exhibit 1

Finding 2: External risks identified relating to regulatory and legal issues are mitigated substantially by (a) Microsoft's agreement to use model contract binding clauses, and (b) consideration that issues identified as potentially material (e.g. US patriot act), are very substantially represented by current risks, and (c), Microsoft's agreement to hold EU data within the EU for specific services (Sharepoint and email). Microsoft Onedrive data is held in compliance with EU data protection law, but is not necessarily hosted within the EU.

Finding 3: The key risks of adoption identified are (a) the act and process of data migration where sharepoint services are adopted, (b) the hosting of data with a single external vendor- consideration should be given to archiving data with a different 3rd party to facilitate future out-migration from Microsoft, and (c) the management of the Microsoft environment and related provisioning, management, auditing and integration with existing and future services.

Finding 4: Adoption of Microsoft services does not mitigate a variety of information security risks to which UCD is currently exposed, notably in the areas of protecting high assurance material, end user account compromise, and potential data leakage from endpoint loss or theft. This would equally be true of any alternative service, but the adoption offers the opportunity to maintain control over sensitive material that may currently be susceptible to elevated risk.

RECOMMENDATIONS

Recommendation 1: It should be assumed that there exist documents and sets of data that should remain within UCD's sole control while hosted or transmitted over Microsoft's infrastructure. Commercial Solutions for high assurance overlays (Information Security rights management systems) on the Microsoft cloud framework for sensitive\high value data should be reviewed for use by the relevant UCD user communities. In particular, UCD should evaluate potential market solutions in this area for storage of medical records, ethically sensitive resources and any materials held with strict confidentiality obligations involving liability for disclosure.

Recommendation 2: IT Services should consider selecting a separate service for document\record archiving for any email\document archive services required. This will mitigate the risk of a single external supplier hosting all such data, and facilitate any future exit strategy.

Recommendation 3: IT Services should conduct a periodic review of Information Risk Governance across the hosted services, as Microsoft's platforms have an extensive base of functionality and services, any of which may have adverse implications for the security of data hosted.

Recommendation 4: Define an information assurance framework for services that integrate directly with UCD's Microsoft services – e.g. Audit systems, eDiscovery, 3rd party services on the Azure platform.

Recommendation 5: IT Services must define new formal policies to manage issues native to the Microsoft platform in the areas of user provisioning and removal, data ownership and sharing.

Recommendation 6: Complementary systems related to UCD's use of Microsoft should be assessed to meet current and emerging risks in the areas of information theft and account abuse. These include user account creation and provisioning, mobile device management, and device\file\cloud encryption services.

Recommendation 7: UCD should maintain security based relationships with other Office 365 customers for the purposes of shared learning arising from incidents in this environment.

Recommendation 8: UCD internal systems related to the Microsoft environment require additional development to meet the requirements of external hosting- e.g. audit capabilities on single sign-on infrastructure, service availability testing for Microsoft services.

BASIS OF ASSESSMENT

This document proposes to establish trust and confidence by UCD in the control of data hosted by Microsoft. Using a set of appropriate industry standard frameworks- the Cloud Control Matrix (CCM), ISO 27001 and audited external reviews (SSAE 16), we seek to establish that controls in place in Microsoft and proposed for UCD meet the standards of best practice in data security and control.

Secondly, we review existing and proposed data protection regulation and review UCD's options in achieving regulatory compliance while receiving the benefits of using a cloud services based approach to email service hosting.

Third, preliminary discussion and external reference material is listed for legal issues around requirements to supply data on the basis of government requirement.

Finally, a series of recommendations (listed above) are proposed for IT Services to consider in achieving regulatory compliance and effective risk management in the use of cloud services, in negotiations with proposed suppliers, and as technical options to address anticipated gaps between UCD requirements and services available from Microsoft's standard service offering.

BACKGROUND- SECURITY STANDARDS

Cloud service providers face a key challenge in demonstrating responsible security management to current and potential customers on a global basis to thousands of clients. Their goal in this case is not only to ensure that customer data is secure, but also that this is demonstrable in some manner which provides assurance to customers while not allowing them to conduct their own audits- a significant drain on resources that should be committed to securing systems. .

In response to this, Cloud Service providers have adopted a number of existing and emerging Security standards, and are audited to those standards by independent 3rd parties in a verifiable manner. Some of these standards (ISAE 3402, 27001) represent those audit statements, while others (CCM, ENISA Assurance framework) represent self-certification statements in that they are prepared and provided by the suppliers themselves according to requirements stipulated by the bodies involved.

THE CLOUD CONTROL MATRIX

The Cloud Control Matrix (CCM) is published by the Cloud Security Alliance- a not-for-profit, member driven organisation of leading security practitioners focused on establishing appropriate criteria for decision making when considering a cloud service provider. The matrix provides a detailed understanding of security and privacy across 13 domains, each of which is also aligned with controls and practices from industry (e.g. CoBIT, ISO 27001),

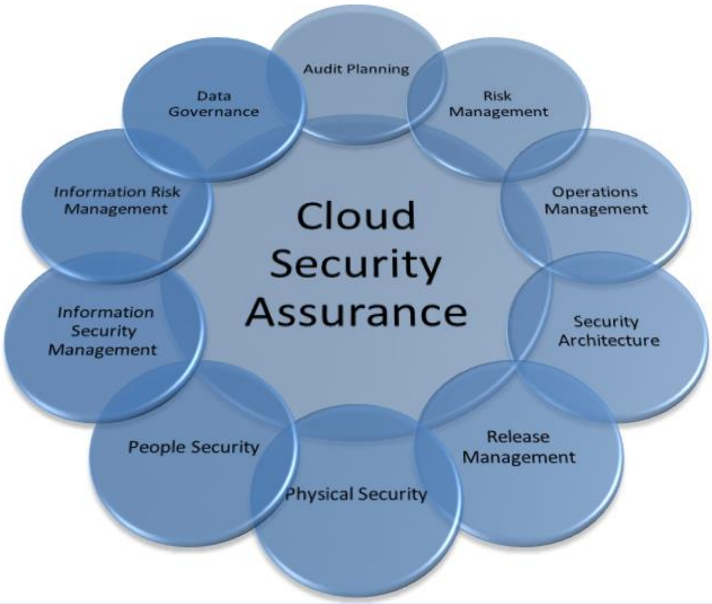


Figure: Cloud Security Alliance CCM Framework Domains.

ISO 27001

ISO 27001 is a standard for Information Security management that allows organisations to establish an Information Security management system to achieve a demonstrable level of commitment to the management of risks associated with managing the Availability, Confidentiality and Integrity of Information systems. Both Google and Microsoft (among others) have achieved compliance with this standard for their public cloud services.

SSAE 3402

SSAE 3402 was developed to provide an international assurance standard for allowing public accountants to issue a report for use by user organizations and their auditors (user auditors) on the controls at a service organization that are likely to impact or be a part of the user organization’s system of internal control over financial reporting. It came into effect in June 2011, replacing SAS 70. Microsoft has provided copies of these reports in their US version (SSAE 16) to UCD, subject to Non-Disclosure Agreement (NDA).

CLOUD SECURITY ALLIANCE

The Cloud Security Alliance (CSA) is an industry alliance comprising service providers, assurance and security service companies. The alliance has developed assurance standards and frameworks for compliance (collectively called the CCM) designed to provide to assurance to users of compliant services that the services provided conform to high standards of service provision, security and trust.

The CSA framework draws heavily from the ISO 27001 standard, and Microsoft has adopted the framework as a mechanism to propose security compliance in Europe as a publicly disclosed counterpart to SSAE control audit statements. A copy of Microsoft’s CSA CCM (Cloud control Matrix) assurance framework response has been provided to UCD.

APPROACH

IT Services has reviewed the proposed adoption of Cloud based email services against a set of criteria built from an enterprise risk assessment viewpoint. Initially, we review the environmental factors that contribute to the decision to adopt a cloud service provider, and assess the risks associated with migration to such an environment.

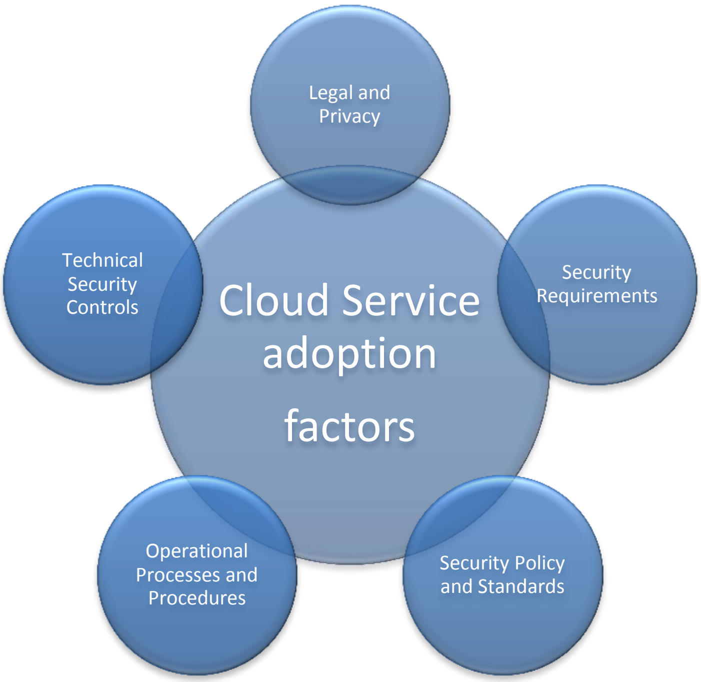

Legal and Privacy
Technical Security Controls
Cloud Service adoption factors
Security Requirements
Operational Processes and Procedures
Security Policy and Standards

Figure 1: Cloud adoption assurance factors

TECHNICAL SECURITY CONTROLS

Organisations that use cloud services have a responsibility to control and maintain their environment once the service has been provisioned. Therefore any consideration of the security requirements for a cloud based service must also consider the residual impact on the UCD's security controls. In particular, user provisioning, access management and incident management mechanisms must be in place, supported by appropriate policies and procedures for overall risk management, in accordance with their regulatory requirements. This is illustrated by the high level architecture below, showing the spread of technical elements colour coded by areas of responsibility. The framework is applicable to both UCD and Microsoft's service provision architectures.

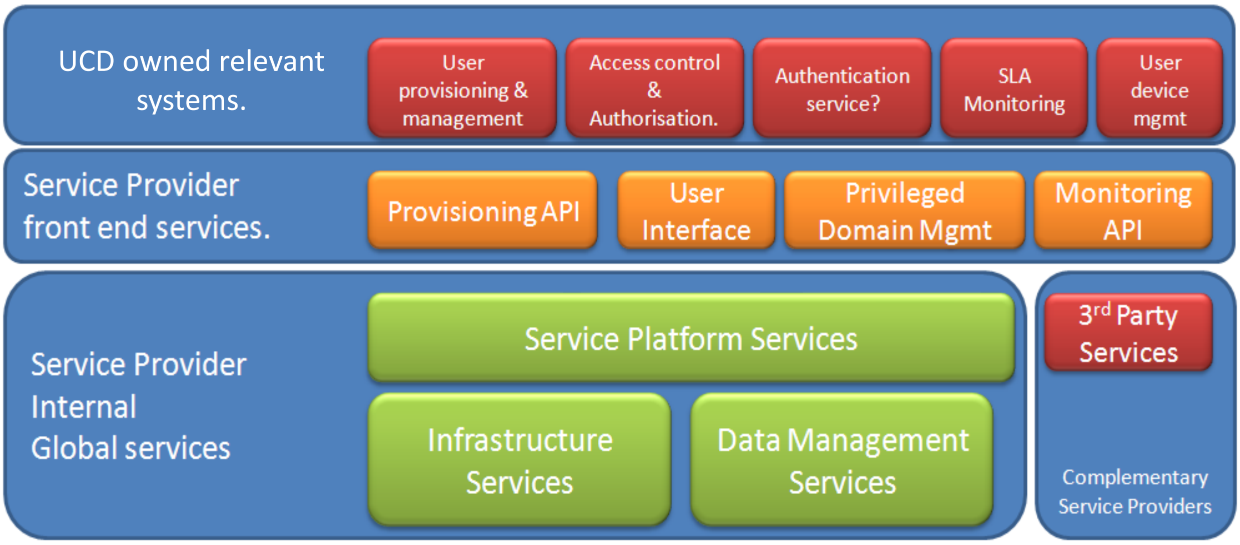

UCD owned relevant systems.
User provisioning & management
Access control & Authorisation.
Authentication service?
SLA Monitoring
User device mgmt
Service Provider front end services.
Provisioning API
User Interface
Privileged Domain Mgmt
Monitoring API
Service Provider Internal Global services
Service Platform Services
Infrastructure Services
Data Management Services
3rd Party Services
Complementary Service Providers

Figure 2: Cloud Services High Level Architecture

Systems shown in red above represent existing or required internal systems that provide data and\or services necessary for the secure operation of the cloud-hosted service. Other systems identified as red in the schematic above include 3rd party service providers- in general, these may be complementary service providers integrated with the cloud service offering (e.g. Email archive\spam filtering providers), or 3rd parties associated with primary service provision.

In the UCD case, Microsoft own and operate their respective infrastructures and where outsourced services are used, their scope is limited and also managed within the scope of the secured managed service. The only 3rd party services potentially in scope are those specifically purchased to integrate with the cloud service provider's service offering.

Systems shown in orange above are usually services hosted by Microsoft, but operated and administered by UCD staff. These services are critical to management of security as they define the customer-specific control and access framework for services provided by Microsoft, and are the primary mechanisms through which UCD asserts control over the data for which it is responsible. In the Office 365 case, this architectural reference point reflects the Interface between UCD Active directory and the Microsoft Azure Domain associated with UCD's tenancy, through to the Office 365 Administrative interface.

Systems shown in green above are internal to the cloud service provider (CSP) and are the applications, platforms and infrastructure that collectively deliver the CSP's service. Operational oversight of these systems is not possible from the customer perspective, and the services provided at this level, together with the front end services, form the basis of assurance in the scope of security certifications. In the Microsoft case, this environment is opaque to all UCD users, and limited API functionality is available to source data from this tier.

"RED" SYSTEMS REVIEW

UCD have conducted a preliminary security review of the Microsoft Office 365 service, and a corresponding exercise at a wider level on the implications for security of documents hosted in the public cloud. These review findings have focused on the practical problems of establishing a like for like control framework for data entering and leaving the system, and the practical problems of sharing data across the enterprise space.

As per the figure above, IT Services' internal risk assessment has considered the elements of the overall service that reflect the requirement to address risks that meet or exceed current capabilities. Examples of these are shown below, and this assessment will continue and expand following a decision to proceed with integration\migration.

Item	Key risk\requirement	Current control	Risk control in the cloud
End User provisioning	Access to the contents of user accounts must be limited to those who are authorised by UCD.	UCD's Identity management system automates end user provisioning based on IDMS records. In the Novell environment, Data owners must request lists of users with current access to the data they are responsible for.	End user provisioning for cloud services remains integrated with UCD's Identity Management framework along current lines. Data owners should be provided the facility in the UCD IDMS to audit current holders of roles entitling them to access the assets they control or manage. This can be provided either though bespoke functionality on the IDMS, or through the Office 365 admin dashboard. Microsoft's Office 365 environment is built with standardised and default policies on sharing data within a tenancy – e.g. internal directories and contact lists. It should be assumed that this will have some feature interaction with personal repositories of current outlook users, data sourced from social networks, data sourced from mobile devices on which clients are installed (e.g. Lync) and standard features of enterprise deployments that may result in unanticipated sharing of personal data within the UCD tenancy sourced through the provisioning system. This should be mitigated through testing.
End user access	Data may be downloaded to uncontrolled devices. Internet access to these services is available from the internet on a number of application ports	Access to UCD group shared data is limited to users provisioned on the Novell fileshare environment. Current web-based access methods have limited utility. Incidents are rare. Operational data is routinely downloaded to end user devices and is dependent on the implementation of endpoint encryption. .	Overall, this is a risk-neutral change. Microsoft's Sharepoint online offering provides equivalent functionality in security terms to the current Novell environment, with additional functionality of value to UCD users (direct integration with Office suite, controls on external sharing etc.) In the UCD case, we will require a baseline policy that defines all document libraries set up in Sharepoint to have a default access level of internal (i.e. no external sharing), in addition to group provisioning. Data owners must request that their document libraries be capable of external sharing. Note that it appears that such sharing with named users is limited to 500 individuals per tenancy, and so this feature will require review before deployment.

			Sharepoint mitigates the requirement to retain downloaded copies of documents, but onedrive encrypts data at rest only in Microsoft datacentres and in network transit. Microsoft and other endpoints require dedicated endpoint encryption to protect data at rest in the user domain.
Security\Event monitoring	Incidents and security relevant events on hosted services must be recorded and used to facilitate operational risk management.	Current systems have internal mechanisms in place to monitor and manage incidents.	Microsoft have extensive logging facilities available in the sharepoint domain, derived from document management, versioning and control. This will require further review and policy determination to assess. In the case of One drive, extensive changes in the product have resulted in an unclear level of functionality in this space, and administrative oversight of this functional space is limited at present. Overall, Microsoft's approach to security events is driven on a per-platform basis, and
Administrative access to data.	Administrative access to hosted data and services must be controlled within UCD.	UCD have an existing function responsible for the management of the email environment.	The tasks associated with UCD's management of the cloud service will require the continued existence of internal support functions. In addition, development resources may be required to facilitate deployments of sharepoint functionality to meet certain business needs.
Authentication	Access to Microsoft services must be via an authenticated channel for end users.	Microsoft use proprietary XML based languages for provisioning, authentication and authorisation, used for interoperability with industry standard SSO and provisioning tools. Microsoft have committed to industry standard SAML support in clients by Q4 2014	These methods will continue for Staff and student access to Microsoft. Federated login events must be tracked for security purposes- a new system is required to facilitate this.
End user devices	Compromised accounts may have all data harvested.	Incidents of this type are currently routine. Current control is to quickly respond to reported incidents of account compromise	Microsoft provides extended logging mechanisms to facilitate potential identification of brute force login attempts. This risk is to some degree adversely impacted by a migration to Microsoft

		and disable access. Account credential quality is low (required minimum quality of passwords is low).	services, simply from the perspective that users will have more convenient remote access to data- if extended authentication methods were adopted or baseline user password standards were improved, this risk would be reduced. In addition, both Microsoft and Google provide mechanisms to support end device encryption and data protection. While not strictly within the scope of the service, they are UCD's second most common source of data loss events.
3rd Party Services	3rd party service providers may have privileged access to data, yet not manage risks as effectively as Microsoft	3rd party service providers are subject to review prior to being provided access to UCD's systems and data. No similar framework has been established for access by 3rd parties via Microsoft's service integration methods.	There are no planned extended services in the Microsoft domain, but this risk should be monitored where such services are proposed.
Tenancy Oversight functions	UCD has requirements to facilitate internal or externally mandated access to individual data under UCD policy	UCD has administrative access\authorised access mechanisms and procedures in place for authorised staff.	Office 365 provides access to an eDiscovery suite of tools for administrative users. Access to this functionality must be strictly limited within the IT Services function to authorised users whose activities in these areas are also logged.

"ORANGE" SYSTEMS REVIEW

Review of the provisioning and account management services available to UCD shows that significant features and capabilities of the Microsoft platform will require policy-level decisions on several matters. The following are recommended from a security perspective:

- End users should not have discretion to make material internet-accessible directly, or by default (e.g. calendar, document sharing).
- End users should not be provided access to all services - only those services explicitly supported by IT Services will be enabled on the service.
- Privileged domain management and provisioning should only be available via the UCD network.
- UCD should deploy an authorisation and audit service to manage and review incidents on the Office 365 environment, based on integration with available monitoring API functionality.
- Documents and other shared materials in the Office 365 environment remain with the owner's account and are deleted when the owner account is removed (regardless of share status). De-provisioning users in this case carries risks of institutional data loss, and this needs to be factored into service design, but likely policy options each have drawbacks. The current UCD strategy of delegated ownership will mean that personally managed documents (for example in onedrive) will continue to reside on personally owned equipment, but deleted from UCD's enterprise environment.

Careful consideration should be given to forms of delegated ownership to be made available to senior managers and record holding functional areas across UCD.

"GREEN" SYSTEMS (CLOUD SERVICE PROVIDER) REVIEW

These are the "Green" and "Orange" systems above, which substantially fall behind the veil of CSP security. Microsoft have provided extensive materials, some subject to Non-Disclosure agreement, that provide extensive information and assurance, and has received independent certification in information security from a number of independent 3rd parties competent in the assessment of technical security, and have established compliant operations against a range of specified controls that represent best practice in Information Security Management. From an operational procedural standpoint, it is accepted that these standards meet UCD's internal requirements for operational security practice. The materials provided\available for review from Microsoft include:

Standard	Microsoft	UCD Comments
ISO 27001	Yes- independently audited	Microsoft have certified the Microsoft Online environments environment to ISO 27001 as part of their compliance programme. The scope of implementation covers the services proposed for use by UCD, and provides independent surety in respect of the CCM framework above. This assurance covers Microsoft's datacentres (Microsoft Global Foundation Services), Platforms (Microsoft Azure) and The Office 365 Platforms (Microsoft Online Services). Each of these certifications have been reviewed.
SSAE16 SOC1 Certification	Yes-Independent assessment available under NDA	Microsoft's SSAE certification is complete, (with some routine exceptions noted). This form of control provides, on the basis of sampling and other assessment methods, evidence to assure that a set of claimed controls is in place and effective for a given period. The set of controls are similar to those above for 27001 and the CCM Framework. This assurance covers Microsoft's datacentres (Microsoft Global Foundation Services), Platforms (Microsoft Azure) and The Office 365 Platforms (Microsoft Online Services). Each of these reports been reviewed. The SSAE is designed to be equivalent to a statement of audited accounts for control of a systems environment, including the potential for litigation in the event that audit control statements are found to be not in place or effective for a given period.
HIPAA BAA	Yes	Microsoft's standard assurance mechanisms permit Microsoft to sign a HIPAA BAA with UCD.
CSA (Cloud Security Alliance)	Yes	Microsoft have disclosed a self-certified set of controls for the Office 365 environment and related infrastructures through the CSA assurance programme.

NOTE ON MATERIALITY OF SECURITY ASSURANCE STATEMENTS.

The security assurance statements from organisations that issue SSAE16 certifications, though effective in establishing the presence of controls in a given organisation, do not provide guarantees that incidents will not occur that might adversely impact the customer. They also represent a commitment by the auditor that has some binding context in litigation should a customer depending on the control statement be sufficiently adversely impacted by an incident i.e. the customer may involve the assurance provider in litigation with a service provider.

Accordingly the statements of assurance are specific in the scope of assurance they provide, and should be interpreted with a high degree of precision. Control statements identify the existence of a control and note exceptions. In financial statements the level of incident that is regarded as an exception is defined by a concept of "materiality" – a cost or impact equivalent to a dollar figure. The level of materiality applied to a particular control report relating to the effectiveness of a system control should therefore be identified as part of the assurance process.

For this reason, for internal purposes, we need to satisfy ourselves that a serious incident material to an organisation like UCD should also be reflected in some form of external reporting from Microsoft - i.e. if another organisation suffers an incident related to Microsoft service use which would materially impact or force UCD to review continued use of that the Microsoft platform, this should be reflected in the audit material available to UCD. Microsoft has committed to report such incidents impacting UCD directly, but incidents relevant to UCD that impact other tenants will not be reported via Microsoft. For this reason, UCD should maintain security based relationships with other Office 365 customers for the purposes of shared learning in this environment.

SECURITY REQUIREMENTS

IT Services have defined a high level set of Security requirements, as necessary to facilitate the vendor selection process, which requires that the service be well managed and secure according to the criteria established in external standards, primarily ISO 27001. In addition, a significant goal of this project is to assess whether Office 365 is suitable for use to store UCD's most sensitive operational data- classified as "Red" or "Strictly confidential" data (HR records, Health related research data etc.) This represents the high watermark level for data managed at UCD.

DATA CLASSIFICATION, OWNERSHIP AND ENCRYPTION

Every organization has highly sensitive and valuable information, from financial documents, engineering intellectual property to personal employee and customer information. IT Services has recognised that such data exists in the UCD shared storage environment, but also that subsets of what is considered highly sensitive data is also transferred within this environment, which presents additional risk when deployed in an external environment. It is prudent, therefore, to consider additional security mechanisms to limit exposure of these materials in the event of a cloud compromise event.

It is technically feasible, even for relatively large groups of users, to securely share highly sensitive materials, even outside the context of a given organisation. While not appropriate for the majority of users, UCD should consider deployment of an overlay rights management system to ensure documents and emails containing operationally and strategically sensitive information is positively controlled, even within the context of a well-regulated hosted email system. These options include file level encryption technologies that are linked to existing enterprise directories, and are compatible with a range of potential use cases, with the following objectives:

- Retain control of sensitive information, even after it has been shared

- Track documents and emails forwarded to internal and external audiences
- Prevent unauthorized access to, extraction from, or editing of information
- Revoke information access when business relationships change, or retention policies require destruction
- Implement policy based controls that allow rights to be stipulated and associated with content, even dissociated from a network.
- Be resistant to deliberate attempts to compromise material, even by technically privileged insiders.

The market for solutions in this space has changed in the past three years, as some secure endpoint solutions (device encryption) have migrated to encompass this capability, in addition to existing companies like Adobe, Oracle and Microsoft. In this case, UCD should consider deploying a solution that protects data across all devices and cloud, rather than adopting a point solution.

CONTRACT TERMS AND DATA MIGRATION- HOW DOES IT END?

In this section we consider the cloud providers in the data migration sense of the technical controls over passing and returning data from UCD to the CSP, in particular the migration processes associated with out-migration from the office 365 service. In Microsoft, substantial capabilities and facilities have been put in place to enable in and out-migration of customers from the service provider, and the company has made clear in the terms of service that it has no rights or ownership or controller status for data held.

Microsoft has defined the methods by which data is removed from their systems, and it should be noted that, this is an explicit deletion process. UCD will be provided with an option for data export, and data is guaranteed to be deleted within a period not exceeding 180 days from the date of service termination. Such out-migration may be accomplished using freely available (but generally commercially licensed) data migration toolkits.

From a risk and compliance perspective it should be noted that public-quoted companies are required to retain document archives for executives and senior managers. Other organisations do so for all staff. This has created a sustainable market for these services in the context of cloud service providers, and UCD should consider this requirement, as it also significantly mitigates risk in the case of a decision to out-migrate at some future date.

THIRD PARTY SUPPLIERS- INTEGRATING OTHER PRODUCTS

Third party suppliers represent a significant consideration for Cloud service offerings, in particular partner suppliers that provide complementary services to the cloud offering.

Outsourcing enterprise applications to the public cloud often involves the identification of technical or procedural gaps that must be resolved using additional services from Microsoft or integrated service suppliers.

In all cases it should be borne in mind that such 3rd party services do not fall within the scope of protected infrastructure, and must usually be assessed separately in their own right as a potential service provider. Microsoft have no 3rd party services at this time that UCD is considering adopting.

IT Services needs to define a process for adoption of new services within the cloud services framework. In many cases, adoption of new services may appear simply as a new feature on the platform, yet offer back-door access to the UCD environment to a 3rd party. Secondly, such services integrate for provisioning purposes with the cloud environment, and may (for example) generate federated identity credentials, or gain privileged access to UCD data. These methods are most notably possible through OAUTH frameworks, which Microsoft does not support.

LEGAL AND PRIVACY

The key legal factor potentially associated with cloud service adoption for UCD staff and potential extended adoption of Cloud based services from global service providers is Data Protection legislation and related regulation.

DATA EXPORT

In Ireland, Section 11 of the Data Protection Acts 1988 and 2003 specify the conditions that must be met before personal data may be transferred outside the EU. Organisations that transfer personal data from Ireland outside the EU will need to ensure that the country in question provides an adequate level of data protection. Some third countries have been approved for this purpose by the EU Commission. The US 'Safe Harbour' arrangement has also been approved, for US companies which agree to be bound by its data protection rules.

In the case of countries that have not been approved in this way, there are a number of other ways in which a data controller can ensure that the data protection rights of individuals are respected. The Controller can use EU-approved model contract clauses which contain data protection safeguards to EU standards, suppliers can establish binding corporate rules, or users can provide consent. Other provisions exist for transfer of data relating to criminal matters and justice co-operation, but these are limited in scope and not relevant here.

Microsoft have adopted the model contract clause mechanism to facilitate global compliance with EU data protection law, in addition to the US\Swiss safe harbour frameworks, in addition to retaining certain classes of UCD data within the EU (i.e. Sharepoint data).

DATA OWNERSHIP AND GOVERNANCE

For enterprise services, Microsoft does not establish any form of controller relationship or ownership of data held for UCD under the service agreement. The service agreement in place at July 2014 will not be superseded by subsequent agreements for UCD during the lifetime of the UCD tenancy, unless additional terms are agreed arising from the adoption of additional services.

Microsoft is established in the EU in Ireland, and contracts are established in the EU. The company has stipulated commitment to meeting EU regulatory obligations as part of their Assurance statements[3].

In addition, the EU Data protection Working group has approved Microsoft's standard model contract terms for Data protection compliance in the EU.[4]

LEGAL INTERCEPT AND DATA JURISDICTION.

Much discussion has taken place regarding the impact of the US Patriot act and related legislation. In addition, the Edward Snowden's release of classified material has shown that the governments of the US, UK, Canada, New Zealand and Australia in particular, have maintained an active, extensive and systematic programme of capture of internet traffic, internal traffic of ISPs, and access to the data repositories of Cloud service providers within the US and internationally. This form of surveillance has come to be regarded as an attack on the

[3] Microsoft Online terms of Service, July 2014- Listed in references.

[4] See Article 29 Working group approval of Microsoft terms (29 April 2014) Listed in references

Internet by the Internet Engineering community[5]. The outcome of this review means that the technical underpinnings of primary Internet services, over time, will evolve to be more resistant to this form of monitoring.

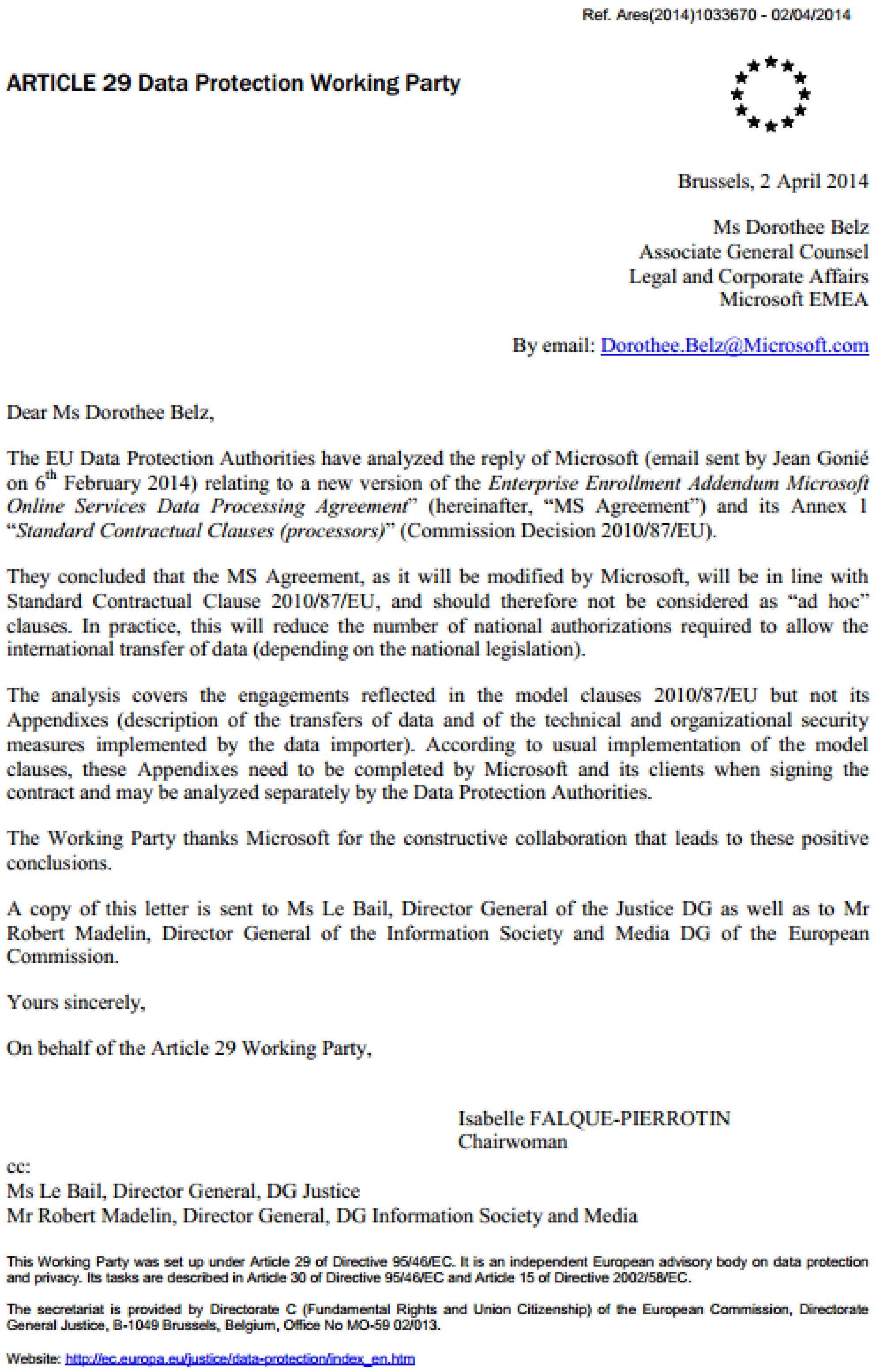
While detailed review of these issues is beyond the scope of this report, independent legal material[6] describes cases showing that US Legislation in the area of data monitoring is not especially different in scope from existing requirements under anti-terrorist legislation in Europe. Within the EU, mechanisms exist across territorial boundaries under Justice “Mutual Assistance” treaties for state security and criminal matters. Entities with requirements to maintain information security capability adequate to defeat or attenuate oversight or intrusion from a competent and resourced adversary are beyond the scope of UCD’s mainstream requirements.

[5] See IETF RFC 7258 “Pervasive monitoring is an Attack” (Stephen Farrell)- listed in references.

[6] See “Law enforcement and Cloud computing” listed in references.

EXHIBIT 1 – EU DATA PROTECTION ARTICLE 29 WORKING GROUP

The Artice 29 working group was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC, and represents a collective view of EU Data protection authorities.



Ref. Ares(2014)1033670 - 02/04/2014

ARTICLE 29 Data Protection Working Party

Brussels, 2 April 2014

Ms Dorothee Belz
Associate General Counsel
Legal and Corporate Affairs
Microsoft EMEA

By email: Dorothee.Belz@Microsoft.com

Dear Ms Dorothee Belz,

The EU Data Protection Authorities have analyzed the reply of Microsoft (email sent by Jean Gonié on 6th February 2014) relating to a new version of the *Enterprise Enrollment Addendum Microsoft Online Services Data Processing Agreement*" (hereinafter, "MS Agreement") and its Annex 1 "*Standard Contractual Clauses (processors)*" (Commission Decision 2010/87/EU).

They concluded that the MS Agreement, as it will be modified by Microsoft, will be in line with Standard Contractual Clause 2010/87/EU, and should therefore not be considered as "ad hoc" clauses. In practice, this will reduce the number of national authorizations required to allow the international transfer of data (depending on the national legislation).

The analysis covers the engagements reflected in the model clauses 2010/87/EU but not its Appendixes (description of the transfers of data and of the technical and organizational security measures implemented by the data importer). According to usual implementation of the model clauses, these Appendixes need to be completed by Microsoft and its clients when signing the contract and may be analyzed separately by the Data Protection Authorities.

The Working Party thanks Microsoft for the constructive collaboration that leads to these positive conclusions.

A copy of this letter is sent to Ms Le Bail, Director General of the Justice DG as well as to Mr Robert Madelin, Director General of the Information Society and Media DG of the European Commission.

Yours sincerely,

On behalf of the Article 29 Working Party,

Isabelle FALQUE-PIERROTIN
Chairwoman

cc:
Ms Le Bail, Director General, DG Justice
Mr Robert Madelin, Director General, DG Information Society and Media

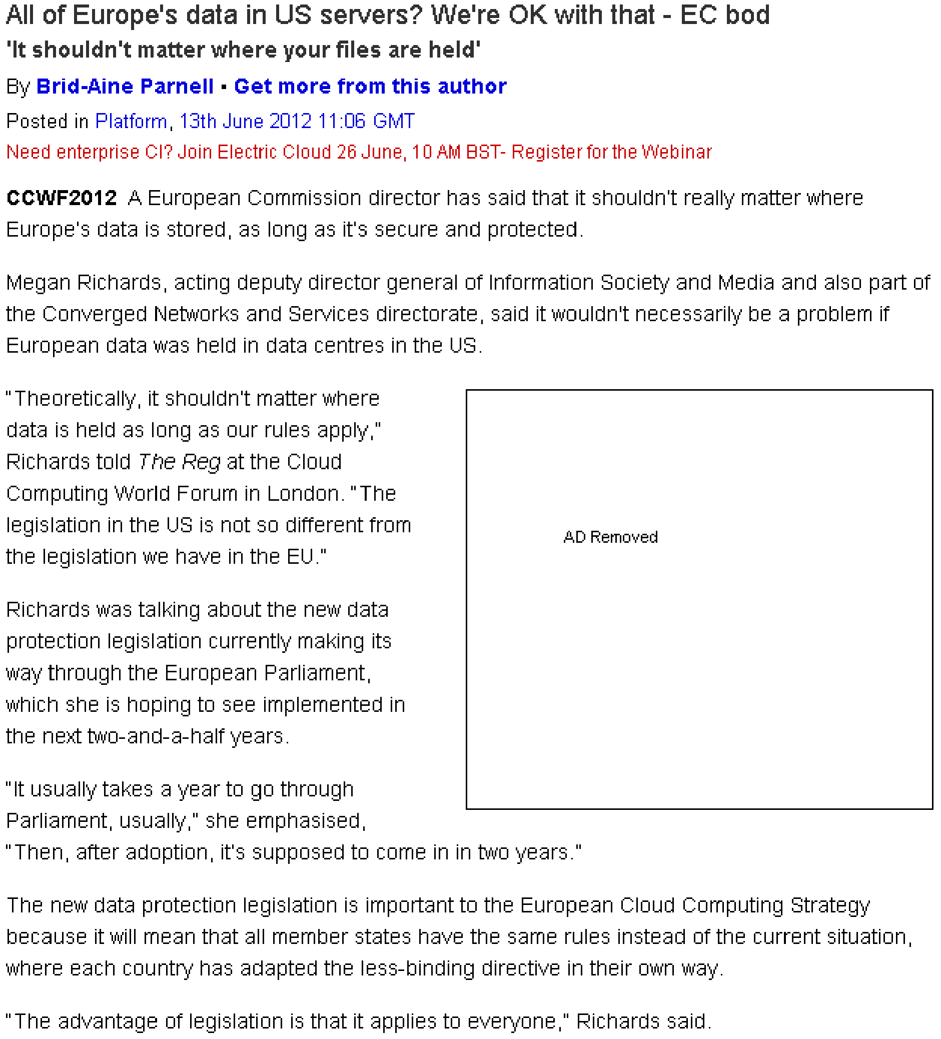
This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013.

Website: http://ec.europa.eu/justice/data-protection/index_en.htm

EXHIBIT 2:

All of Europe's Data in US servers? We're OK with that- EC bod
(From The Register- http://www.theregister.co.uk/2012/06/13/ec_cloud_data_anywhere/)



All of Europe's data in US servers? We're OK with that - EC bod

'It shouldn't matter where your files are held'

By **Brid-Aine Parnell** • **Get more from this author**

Posted in Platform, 13th June 2012 11:06 GMT

CCWF2012 A European Commission director has said that it shouldn't really matter where Europe's data is stored, as long as it's secure and protected.

Megan Richards, acting deputy director general of Information Society and Media and also part of the Converged Networks and Services directorate, said it wouldn't necessarily be a problem if European data was held in data centres in the US.

"Theoretically, it shouldn't matter where data is held as long as our rules apply," Richards told *The Reg* at the Cloud Computing World Forum in London. "The legislation in the US is not so different from the legislation we have in the EU."

Richards was talking about the new data protection legislation currently making its way through the European Parliament, which she is hoping to see implemented in the next two-and-a-half years.

"It usually takes a year to go through Parliament, usually," she emphasised, "Then, after adoption, it's supposed to come in in two years."

The new data protection legislation is important to the European Cloud Computing Strategy because it will mean that all member states have the same rules instead of the current situation, where each country has adapted the less-binding directive in their own way.

"The advantage of legislation is that it applies to everyone," Richards said.

REFERENCES AND BIBLIOGRAPHY:

Links are provided for publicly available material where possible. Exhibits are provided as background material, and in original text as media news sites are more likely to change URL.

DATA PROTECTION LAW AND REGULATION

1. Regulatory considerations in data transfer.
   (FAQ available for download at:
   http://www.dataprotection.ie/ViewDoc.asp?fn=/documents/responsibilities/3ma.htm&CatID=56&m=y)
2. EU Model Contract Clauses- revised 2010
   (Available online at:
   http://ec.europa.eu/justice/policies/privacy/docs/modelcontracts/c_2010_593/c_2010_0593_en.doc
)
3. Article 29 Working group legislative proposal (General Data Protection Regulations) (Available at:
   http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF
4. "Law Enforcement and Cloud Computing" - Linklaters law firm paper on European legislation in relevant areas (October 2011). Available from IT Security (no longer available for download)
5. Article 29 Working group approval of Microsoft terms (29 April 2014) :
   http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140402_microsoft.pdf

MICROSOFT OFFICE 365 SECURITY

6. Microsoft Volume Licensing Online Service Terms (Worldwide English, July 2014).
   http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=31
7. Microsoft Office 365 Security and Compliance (May 2014).
8. Microsoft Online Services ISO 27001:2005 Certification (Available from www.bsiglobal.com)
   a. Office 365 (IS 552878)
   b. Windows Azure (IS 577753)
   c. Microsoft Global Foundation Services Division (IS 587621)
   d. Microsoft Office Online Services -FOPE (IS 552878- UKAS)
9. Microsoft Office Trust center http://office.microsoft.com/en-ie/business/office-365-trust-center-cloud-computing-security-FX103030390.aspx?redir=0
10. Microsoft Information security- Independent Auditor's reports:
    a. Microsoft Global Foundation Services SSAE 16 SOC 2 & SOC 1 reports
    b. Microsoft Azure Services SSAE 16 SOC1 Type II
    c. Microsoft Office 365 SSAE 16 SOC1 Type II
11. Microsoft CSA CCM Compliance statement (Windows Azure):
    https://blog.cloudsecurityalliance.org/2013/08/22/windows-azure-leads-way-with-soc-2-csa-ccm-attestation/

TECHNICAL SECURITY STANDARDS

12. ISO 27001- available through http://www.bsiglobal.com .
13. Cloud Security Alliance Cloud Control Matrix- available through http://cloudsecurityalliance.org
14. American institute of CPA's Principles and criteria for Security, Availability, Processing Integrity , Confidentiality and Privacy-

http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/TrustServices/DownloadableDocuments/FINAL_Trust_services_PC_Only_0609.pdf

15. ENISA Cloud Information assurance requirements- (Available online at: http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-information-assurance-framework/at_download/fullReport)
16. IT Risk: Turning Business Threats into Competitive Advantage – (2007) Westerman & Hunter (Harvard press)

OTHER

17. Google apps versus Microsoft Office 365 at Berkeley: http://technology.berkeley.edu/productivity-suite/google/matrix.html

18. Pervasive Monitoring is an Attack- (Stephen Farrell et al) IETF Document RFC 7258- http://tools.ietf.org/html/rfc7258