InterPARES Trust Project

Research Report

Title:		TR02 – Case study: IFRC*jobs*, a SaaS recruiting tool
Status:		Final
Version:		2.0
Date submitted:		19.02.2016
Last reviewed:		
Author:		InterPARES Trust Project
Writer(s):		Weimei Pan and Grant Mitchell
Research domain:		Control
URL:		

Document Control

Version history			
Version	Date	By	Version notes
0.1	29.08.2015	Weimei Pan	Submitted to Grant Mitchell for comments
0.2	21.09.2015	Grant Mitchell	Edits and comments for Weimei
0.3	11.1.2016	Weimei Pan	Revise the draft based on Grant Mitchell's comments. Finish the rest of the report and submit to Grant Mitchell for comments.
0.4	26.1.2016	Grant Mitchell	Edits and comments for Weimei
0.5	28.1.2016	Weimei Pan	Refine the draft based on Grant Mitchell's comments and finalize the report.
1.0	6.2.2016	Weimei Pan	Finalize the report based on the comments from Grant Mitchell
2.0	9.2.2016	Grant Mitchell	Final edit before submission for IFRC Legal Dept approval

Table of Contents

Acknowledgement

We gratefully acknowledge the assistance the International Federation of Red Cross and Red Crescent Societies and the staff who participated in this study.

Executive Summary

This report provides an analysis and evaluation of a public-cloud based Software as a Service (SaaS) recruitment application—IFRC*jobs*. It aims to examine how various issues related to the use of cloud-based services are addressed in practice and to provide empirical input to related InterPARES Trust projects. Multiple methods have been used for data collection, including semi-structured interviews, contract analysis, and policy analysis.

The research draws attention to the fact that the introduction and use of cloud-based services involves an integrated set of strategy, roadmap, policies, and tools. Collaboration between different stakeholders in a business, e.g., legal department, IT department, business department, and archives and records management department, is essential in order to effectively protect the organization from any potential risks associated with cloud-based services. Further investigations reveal that archives and records management issues did not receive equal considerations as other issues in the evaluation and introduction of cloud-based services. Their significance is often overlooked. This results in records management issues not consistently and proactively addressed across different cloud-based services. In addition, this research confirms that risk/benefits balance and risk management play a central role in the assessment and introduction of cloud-based services. Related constructs in the management of cloud-based services, such as control, trust, partnership, and monitoring, are also mentioned. Moreover, this research confirms that the nature of cloud-based services poses some unique challenges to international organizations, for instance, the international organization may not enjoy inviolability of archives in the geographical location where the data center is located.

It is recommended:

- that guidelines, and templates for records management in the cloud environment be formulated to assist records managers in managing risks associated with cloud-based services;
- that more research be conducted to investigate the relationship between risk, control, and trust in the management of cloud-based services; and
- that more research be conducted to explore the emerging challenges international organizations are facing in the cloud environment, and any solutions to address these challenges.

1. Introduction

The International Federation of Red Cross and Red Crescent Societies (The Federation) works on the basis of the Principles of the Red Cross and Red Crescent Movement to inspire, facilitate and promote all humanitarian activities carried out by its member National Societies to improve the situation of the most vulnerable people. Founded in 1919, the Federation directs and co-ordinates international assistance of the Movement to victims of natural and technological disasters, to refugees, and in health emergencies. It acts as the official representative of its member Societies in the international field. It promotes co-operation between National Societies, and works to strengthen their capacity to carry out effective disaster preparedness, health and social programs.

The Federation carries out relief operations to assist victims of disasters, and combines this with development work to strengthen the capacities of its member National Societies. The Federation's work focuses on four core areas: promoting humanitarian values, disaster response, disaster preparedness, and health and community care.

In January 2014, the Federation launched a new e-recruitment system called IFRC*jobs*, which is a Software as a Service (hereafter SaaS) application based on public cloud. *IFRCjobs* primarily fulfills three functions: it is a database storing recruitment data and records; it is a business system enabling and supporting recruitment activities and transactions; and it is an electronic recordkeeping system creating and maintaining recruitment records to ensure their evidential value can be protected.

Being a public cloud-based application brings both benefits and issues for IFRC*jobs* to fulfill its three functions. Some of the benefits include economic advantage, scalability, ubiquitous connection, and streamlined and standardized recruitment process. Some of the issues include data security, applicants' privacy, records creation, and retention and disposition of electronic records.

As one of several cloud-based services that the Federation has adopted, the IFRC*jobs* application presents a case for us to explore how organizations evaluate, adopt, implement, and use SaaS applications, how organizations harness the benefits and mitigate the risks of cloud-based services, and how records creation and maintenance are implemented. Another goal of this case study is to provide empirical input to other InterPARES Trust studies by testing the checklist and/or functional requirements drafted by other InterPARES Trust projects and offering recommendations.

2. Data collection and data analysis

Multiple methods have been used to collect data, including policy analysis (e.g. analysis of the Federation's information security classification standard, ICT security policy, and cloud services request form), contract analysis (e.g., terms and conditions, and service level agreement), system assessment (including the documentation of the system functionalities), and semi-structured interviews. Major data collection started in December 2014 and ended in February 2015.

Ten interviews were conducted with staff from the legal department (2), library and archives unit (1), IT department (1), the human resources department (5), and risk and audit department (1). Five interview guides were developed prior to the interview for staff from each department (Appendix A). While in general the interview questions prompted the interviewees to describe how the issues raised by the use of IFRC*jobs* were mitigated and how they utilize its benefits, the interview questions were geared towards the role and responsibilities of each interviewee in the evaluation, adoption, implementation, and use of IFRC*jobs*, and each person's role and responsibilities within the Federation. This will ensure that a comprehensive understanding be obtained of IFRC*jobs*. For instance, the staff from the IT department, who is also the project manager of IFRC*jobs*, was asked to discuss in greater detail the Federation's cloud strategy, the management of the IFRC*jobs* project, contract negotiation, and other issues related to the technology aspect of IFRC*jobs*; by contrast, the staff from the Library and Archives Unit was asked to elaborate more on records management with IFRC*jobs* and other cloud-based applications within the Federation. Each interview lasted between 25 minutes to 90 minutes. Interviews were audio recorded and transcribed afterwards. All personal identifying information was removed for privacy reasons; each interviewee was assigned a unique identification number, e.g., interviewee1, interviewee2.

Products of other relevant InterPARES Trust projects were used as a framework to guide data analysis. The comparison of this case with products of other InterPARES Trust projects and any gaps and discrepancies identified can achieve two purposes: first, it can improve the products of these InterPARES Trust projects by either strengthening their findings or providing evidence to revise their products, therefore, contributing to the overall goal of InterPARES Trust; second, it can offer recommendations to the Federation for modifying IFRC*jobs* and future procurement of cloud-based services.

The comparison with other InterPARES Trust projects was supplemented with independent thematic analysis to identify issues and themes that are not being sufficiently studied by other projects.

3. Background

3.1 Inviolability of Records and Archives

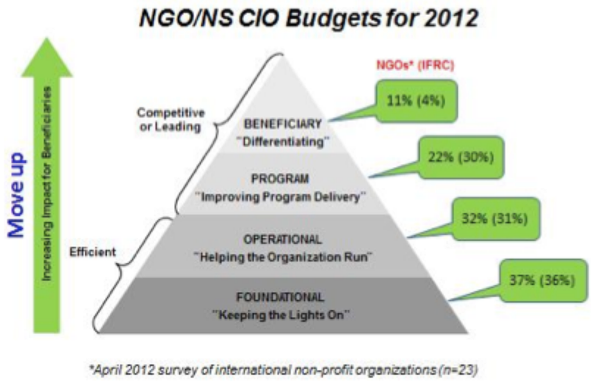
The two principles governing the management of records and archives in international organizations are inviolability of premises and archives, and extraterritoriality (InterPARES Trust Project TR01 Team report 2014). As a type of privilege and immunity enjoyed by international organizations, inviolability comprises four broad types: jurisdictional immunities, inviolability of premises and archives, freedom of communication, and immunity relating to financial matters; among them, inviolability of premises and archives is the principle that "international organizations are accorded a heightened level of protection, so that anyone external to the organization cannot enter the premises or access the archives of the organization unless given express permission or invited to do so" (InterPARES Trust Project TR01 Team report 2015). The principle of inviolability grants international organizations independence and secrecy, which is necessary for them to fulfill their responsibilities (InterPARES Trust Project TR 01 Team report 2015). As to the applicability of the principle of inviolability of archives, this is determined by the following three aspects: it applies to both documents and the information contained in the records; it applies to the archives wherever located (i.e., regardless whether the archives is located in the premises of the organization or not) including when documents are in transit; it applies to records that are either created by the organization or are in the organization's custody (InterPARES Trust Project TR01 Team report 2015).

Although being an international organization, the Federation is not like United Nations agencies, which enjoy universally accepted inviolability of archives; instead, the Federation must negotiate for such inviolability of archives with the government of each country in which it operates. Not every country will grant such inviolability to the Federation. The use of cloud-based services poses many challenges to the execution of this principle. By entrusting the physical custody of the records to the cloud service provider, an issue arises as to how we can ensure and prove that inviolability has been maintained and not circumvented in countries that have granted the Federation the inviolability of archives and how to ensure the trustworthiness of records in countries with which the Federation does not have status agreements granting it inviolability of archives, or in some cases, in countries in which the Federation does not even operate (have an office).

3.2 IT strategy

In April 2012, the Federation conducted a survey of international non-profit organizations concerning the alignment of IT budgets and IT strategy. The Federation measured the IT strategies at four different levels: foundational; operational; program; and beneficiary. Foundational level refers to the computer infrastructure, network, and the various applications that ensure the organization can function; operational level refers to the day-to-day IT services that support IT operations; program refers to the various disaster prevention, disaster relief, or development programs that the organization delivers to its beneficiaries; and beneficiary refers to the use a beneficiary could make of an organization’s IT infrastructure.

The survey results showed that over two-thirds of international non-profit organizations’ IT budgets were spent on the projects at the bottom two levels, i.e., operational and foundational; and only one-third was spent on the top two levels, i.e., program and beneficiary, which are more mission-relevant IT projects, as shown in Figure 1.



*April 2012 survey of international non-profit organizations (n=23)

Figure 1 The alignment between IT budgets and IT strategy in international non-profit organizations (reproduced from IFRC (2012))

Motivated by the result of this survey and other internal and external factors, such as the advancement of cloud computing as a new information technology provision model, the overall strategy of the IFRC, and investment resources, the Federation defined as the essence of their IT strategy getting out the bottom of the pyramid and moving up to the more mission-relevant IT services.

3.3 Cloud Computing Strategy

The Federation started using cloud services very early, but there was not a coherent cloud strategy to leverage the benefits of cloud computing to transform the Federation’s IT capacity. In mid-2012, with the help of a consulting company, the Federation developed their cloud computing strategy and cloud roadmap.

In designing its cloud strategy and roadmap, the Federation assessed the status quo of its IT environment (including the infrastructure level, platform level, and application level), examined the opportunities and challenges offered by the cloud, and presented the target state as measured by the number of applications deployed in public cloud, private cloud, hybrid cloud, and internal dedicated data center. The target state has been assessed in terms of the benefits to be realized (e.g., scalability, ubiquity, cost-effectiveness, availability, resiliency, and performance improvement), and risks to be reduced (e.g., the lack of IT expertise within the Federation, disaster recovery ability, and resiliency of the data center). Though the Federation now prefers to move computer applications to the cloud, it recognizes that there may be applications for which the risks (e.g., legal, financial, and technical) of moving to the cloud are judged too high. The Federation has to balance risks and benefits, and decide what applications to move to the cloud and what applications remain on the Federation's in-house servers.

The cloud roadmap outlines the timeline and the adoption plan of different cloud projects. It also describes the expected benefits and the impact of the cloud services on the organization, in particular, the operating model of the IT department. Moving to the cloud means that the IT department can spend more resources on IT strategy and architecture, and less on service delivery.

The cloud strategy has been reviewed and discussed by different leadership levels of the Federation and stakeholders from different departments (e.g., the Legal department, Risk Management and Audit department, etc.). In addition, a series of templates, forms, checklists, toolkits (e.g., cloud request form, cloud assessment toolkit) have been developed as a result of the Federation's experience in procuring cloud services and are being used for further procurement.

4. The Introduction of IFRC*jobs*

4.1 Balancing Benefits and Risks in Cloud Service Adoption

It is commonly accepted that cloud-based services bring both benefits and risks to the users. Some benefits include scalability, resiliency, and cost-effectiveness. Some risks include data security, privacy, availability, integrity, and legal compliance. Given its status as an international organization, some of the cloud risks much discussed may not be applicable to the Federation, e.g., legal compliance (only in Switzerland). However, the Federation has been striving to comply with Swiss and European data protection legislation and to be on a par with the best practices on data protection.

Given its characteristics, the evaluation of cloud-based services is also a process of balancing the benefits and risks relationship. Organizations usually fall somewhere in the middle along the spectrum of benefits and risks. At the Federation, data related risks are an integral component in assessing and introducing cloud-based services. This is illustrated by the role of the information security classification framework in the evaluation, selection, and procurement of cloud-based services, as interviewee5 confirmed,

> *"[I]t all boils down to the types of data we put in there. This is why data classification became one of the key things we consider, … not only in the cloud request form, but all of the cycle of the product selection."*

By "data classification", interviewee5 was referring to the Federation's information security classification framework, which classifies information into four categories according to their sensitivity level and the possible consequences the Federation may face if the information is not appropriately protected. These four categories are highly restricted, restricted, internal, and public. The framework also outlines the kinds of controls that should be applied to each classification level, and the potential operational and financial impact that unauthorized disclosure, alteration or destruction of data belonging to each classification level could have on the Federation.

At the Federation, information security is defined explicitly in its ICT security policy as "the process of protecting data whether in storage, transit or processing from unauthorized access, use, disclosure, destruction, modification, or disruption whether accidental or international"; it is comprised of three aspects: confidentiality, availability, and integrity. At the Federation, information security is an encompassing concept addressing many data related concerns.

When evaluating an application procurement option, one question the Federation will ask is what types of information are involved in the business functions, transactions, and activities embedded in the application to be procured. For highly restricted and restricted information, for security reasons, it is favorable that the applications remain on the organization's in-house servers. However, this means the Federation would forgo the opportunities offered by the cloud computing to modernize their IT infrastructure, and provide better and more mission relevant IT services. Instead of a blanket ban on using cloud-based services for highly restricted and restricted information, the Federation has generated a more sophisticated cloud computing strategy and roadmap, which allows the Federation to reap the maximum benefits of this new technology provision model. This is realized by properly defining the types of applications that should remain on in-house servers considering the high risk, and the types of applications that can be moved to the cloud if potential risks can be mitigated by due diligence. For instance, the Federation requires that the service provider be based, preferably, first, in Switzerland where the Federation is located, second in Europe, as these two jurisdictions have relatively more stringent data protection legislation. For highly restricted and restricted information, the Federation has to be particularly cautious if the service provider is subject to US legislation, e.g., the Uniting and Strengthening America by providing Appropriate Tools Required to Intercept and Obstruct Terrorism (US-Patriot Act), which gives US law enforcement authorities the right to access data if conditions are deemed as emergency or necessary to homeland security. Nevertheless, doing this would limit the Federation to a small group of choices. In addition to restricting the geographical locations of the service provider, additional restrictions will be placed on the transfer, return, destruction, backup, and protection of data in the contractual documents.

4.2 Motivation for the Adoption of IFRC*jobs*

In the case of IFRC*jobs*, its introduction was partly due to an annual audit performed at the Federation in 2012. The audit results showed that the previous product – also a SaaS application – the Federation used for recruitment had some level of vulnerability. Although the Federation had been positively engaging the service provider to address these vulnerabilities, the efforts were in vain. Another reason is that the previous product was not able to provide a standardized, streamlined, and automatic recruitment process. The previous product was primarily used to collect and store applicants' personal data and related documents, such as CVs; therefore, it has to be complemented with manual paper recruitment process. In addition, the previous product did not have the capacity to integrate with social networks, which reduced the Federation's visibility in reaching a wider range of audiences and attracting high quality and more diverse candidates. Due to the technical vulnerabilities and security risks, and the limitations of the previous product, the Federation decided to replace the previous product.

When terminating the previous recruitment product, measures had to be taken to migrate or dispose of the records stored in the application, mostly applicants' personal data and documents. Most of these data were already out of date, thus having very limited business value. These data were not migrated to existing systems nor to IFRC*jobs* due to the high cost and the limited business value of the data. Yet, for accountability reasons, the Federation negotiated with the service provider for each applicant's data to be converted and provided to the Federation in PDF format. In addition, all the data and the relationships that can be used to recreate the database were returned to the Federation in case the Federation needs to make basic queries, such as, how many applied for certain jobs, how many jobs were posted, and what is the status of jobs.

4.3 Assessment of Proposed Applications

At the time the Federation decided to replace the previous recruitment application, the Federation's cloud strategy and roadmap indicated that the entire recruitment process, including the complete recruitment records, should be moved to the public cloud. Therefore, in the Request For Proposal (RFP) to replace the previous product, it was specifically stated that only cloud-based services would be considered. In addition, it was specified that the new platform should "offer automated workflow management", "integrate with social network mediums", "provide functions to improve analysis of information and aid planning and scheduling to gain in time and efficiency", "allow for flexibility and robustness", "increase the number of qualified applicants", and "increase the number of recruiters worldwide".

From the RFP to the final deployment of the solution, due diligence was performed in each step of the procurement, e.g., comparison and evaluation of the products, cloud request form, legal and IT recommendations, contract negotiation, feature testing, training, communication, problem fixing, and other support services.

The criteria used for the evaluation of the proposed solutions included, but were not limited to, functional requirements (i.e., business needs), non-functional requirements (i.e., IT requirements), legal requirements, finance considerations, and value-added things (e.g., quality of response, the company size, whether the Federation had worked with the provider before, etc.). When evaluating the proposed products, the Federation first examined whether these products had the functionalities essential to the recruitment process, thus, satisfying business needs. As a SaaS application is based on a platform of ecosystems with highly standardized modules, the degree of customization may be limited, and business processes and transactions embedded in the SaaS application are usually generic in nature. As a result, the recruitment process provided by the application may not match perfectly with that at the Federation. This gave the Federation an opportunity to re-examine its recruitment process and determine what were essential and what were just desirable (but not mandatory) requirements.

Once the proposed applications were filtered by how they satisfied the functional requirements, the remaining service providers were asked to answer the questions in the Federation's Cloud Request Form to "uncover legal risks and communicate mitigation or plan of action to reduce or eliminate them" and "to understand the technical applicability and feasibility of using cloud services as the solution". The Cloud Request Form is a form created by the Federation on the basis of its experience in procuring cloud-based services. This form is comprised of three sections: security classification of the information and records involved in the application to be procured, legal considerations, and technical considerations. The legal considerations and technical considerations sections ask the most basic, yet important questions, about the proposed service, for instance, where the service provider is based, whether there is transferring of data from one jurisdiction to another, whether third parties have access to the data, whether the Federation will be notified if there is a security or other breach, whether there are technical and organizational measures to protect data against unauthorized disclosure or access, accidental loss or destruction of data, whether data will be properly removed upon termination of the service, whether the application is taking advantage of cloud hosting, whether the application meets the Federation’s non-functional requirements, and whether the application uses a shared infrastructure for tenants.

By asking these questions, the Federation obtains a basic understanding of the proposed services. The Cloud Request Form along with answers is forwarded to the legal department and IT department for recommendations and comments. Proposed applications that are beyond the Federation’s risk tolerance level are rejected at this round of assessment. The Federation incorporates the recommendations and comments received from the legal department and IT department, along with other issues such as liability, termination of service, and acceptance of product, into its contract negotiations. While each party to the negotiation often starts with a draft contract that favors its interests, the final contract usually is a balance of each party’s interests.

5. Contract Analysis

The contract with the service provider of IFRC*jobs* is composed of five documents: order form, Terms and Conditions (hereafter T and C), Terms and Conditions for other services, Service Level Agreement (hereafter SLA), and Documentation. In addition to these five contractual documents, the following analysis will from time to time refer to the Cloud Request Form, which is not a contractual document, but an internal document used by the Federation to select service provider (See section 4.3). On occasions where relevant information cannot be found in the five contractual documents, information in the Cloud Request Form will be used for the analysis. Since the information in the Cloud Request Form is provided by the service provider, it is assumed that the information is true. However, it is important to note that the Cloud Request Form is not a contractual document.

Since one goal of this project is to provide a "reality check" to "standards of practice" produced by other InterPARES Trust studies, two analyses of the IFRC*jobs* contract have been conducted. One was guided by the Checklist for Cloud Contracts (see Appendix B) drafted by InterPARES Trust research project NA 14 Developing Model Cloud Computing Contracts. This analysis was based on the checklist submitted in May 2015; therefore, it may not be applicable to any subsequent version of the checklist. The other was guided by the Retention & Disposition Functional Requirements (see Appendix C) drafted by InterPARES Trust research project NA 06 Retention & Disposition in a Cloud Environment. This analysis was based on the checklist submitted in March 2015; therefore, it may not be applicable to any subsequent version of the checklist.

The primary purpose of using these checklists was to identify gaps and discrepancies between them and IFRC*jobs* contract. It is hoped that the results of these analyses will provide additional empirical evidence to improve these two checklists. However, the results should be taken with some caution considering the fact that the Federation is an international organization, IFRC*jobs* is a recruitment solution, and the limitation of case study to one computer system.

In addition, the contract was scrutinized against findings of existing studies on cloud contracts to determine its strengths and weaknesses in balancing the relationship between the Federation and the service provider of IFRC*jobs,* and in guaranteeing the services delivered.

5.1 Contract Analysis Using the Checklist for Cloud Contracts

5.1.1 Analysis Results

(1) Agreement

a. *Is the effective start date of the agreement clearly stated?*

Yes. There is a definition of Effective Date in the order form, which is the date when the Federation has signed the order form. The definition also specifies that the contract will commence on the Effective Date.

b. *Is there an explanation of circumstances in which the services could be suspended?*

Yes. According to the T and C, the service provider reserves the right to suspend service provision if the payment of fees is due for more than 30 days and the service provider has sent at least three written reminders. Service may also be suspended if a party (either the Federation or the service provider) is wholly or partially unable to fulfill its obligation under the contract due to Force Majeure.

c. *Is there an explanation of circumstances in which the services could be terminated?*

Yes, but the clauses focus on termination of contract in general, not termination of services. Termination of contract can further be divided into two situations: immediate termination and notified termination; and termination can be initiated by either the service provider or the Federation depending on the cause. According to T and C, reasons for the termination of contract fall into three categories: material breach of the contract, unacceptable use of the service, and a list of exceptional circumstances such as bankruptcy, compulsory insolvency, or Force Majeure.

d. *Is there an explanation of automatic notification, or an option to subscribe to a notification service, in the event of changes made to the terms governing the service?*

Yes. This is covered under the section of Notices in T and C, which describes how notices should be sent. It is assumed that any changes made to the contract are agreed upon by both parties rather than imposed upon the customer by the service provider, as presumed by this Checklist item. Any amendments as agreed by the parties shall be in writing and shall be deemed to have been duly given if sent by registered post or acknowledged fax to a party at the address given for that party in the order form.

(2) Data Ownership and Use

a. *Do you retain ownership of data that you store, transmit, and/or create with the cloud service?*

Yes. T and C states that to the extent personal data is processed using the solutions and service, the service provider is a data processor and the Federation is a data controller. The service provider will only process personal data on behalf of, and in the name of, the Customer. No definition of personal data is provided in the contract. It is not clear whether this clause is only limited to personal data or is applicable to all data stored, transmitted, and/or created with the service.

b. *Does the Provider reserve the right to use your data for the purposes of operating and improving the services?*

Yes. T and C specifies that the service provider can access the Federation's information in the solution for maintenance and support purpose.

c. *Does the Provider reserve the right to use your data for the purpose of advertising?*

Not applicable. This item is primarily associated with free cloud computing services, and is not applicable to IFRC*jobs*.

d. *Does the Provider's compliance with copyright laws restrict the type of content you can store with the cloud service?*

Not clear. The way this Checklist item is phrased makes it more like an internal decision of the customer than a clause in a contract. In addition, the Checklist's reference to copyright may be too specific to address a wide range of rights that may be included in cloud computing contracts. The IFRC*jobs* contract uses Intellectual Property Rights to represent a series of rights, e.g., copyright, patents, design rights, technical information, business names and logos, generic rights, and proprietary rights.

The IFRC*jobs* T and C further addresses the rights related issue by stipulating the responsibilities of the Federation to enable the service provider to fulfill its obligations (e.g., the Federation has obtained data fairly and lawfully, and the Federation has obtained approvals from the data subjects), and indemnities to be made by the Federation if the service provider breaches data protection law or regulations by processing data on behalf of and in accordance with the instructions of the Federation.

e. *Do you gain ownership of metadata generated by the system during procedures of upload, management, download, and migration?*

Contract not clear. No clause on metadata.

f. *Do you have the right to access these metadata during the contractual relationship?*

Contract not clear. No clause on metadata.

(3) Availability, Retrieval, and Use

a. *Are precise indicators provided regarding the availability of the service?*

Yes. Availability, how it is calculated, and how the Federation will be credited if the solution is not available is defined in SLA.

b. *Does the degree of availability of the data meet your business needs?*

c. *Does the degree of availability of the data allow you to comply with freedom of information (FOI) laws?*

d. *Does the degree of availability of the data allow you to comply with the right of persons to access their own personal data?*

e. *Does the degree of availability of the data allow you to comply with the right of authorities to legally access your data for investigation, control, or judicial purposes?*

No. These Checklist items describe the results the Customer can achieve from using the solution. These should be evaluated and determined by the customer. It is unlikely that the service provider will give such warranties in a contract. The IFRC*jobs* contract stipulates, "No warranty is made regarding the results the Customer can achieve from using the Solution and Services nor that the Solution and Services will operate uninterrupted or error free."

f. *Are the procedures, time, and cost for restoring your data following a service outage clearly stated?*

Contract not clear. There is a clause on disaster recovery. If service outage is one kind of disaster, then the recovery procedure is clearly stated.

(4) Data storage and preservation

Data storage

a. *Does the Provider create backups of customer data?*

Yes. T and C stipulates that service will be hosted in the primary data center and secondary data center. The locations of these two centers have been specified in the contract. SLA specifies the backup procedure, the security procedure (the security level in the backup data center is consistent with the main production center), and the retention period of data backups.

b. *In the event of accidental data deletion, does the Provider bear responsibility for data recovery?*

Contract not clear. T and C stipulates that the service provider will immediately notify the Customer of any wrongful deletion of customer data. Though there is no explicit clause on accidental data deletion recovery in the contract, in the cloud request form (which is not a contractual document, but a document used to select service provider) the service provider specifies that in case of deletion, data can be recovered from the backups.

Data preservation

c. *Are there procedures outlined to indicate that your data will be managed over time in a manner that preserves their usability, reliability, authenticity, and integrity?*

No. No clauses on long-term preservation of data. The solution is a business system rather than a records management system; therefore, it is not designed with long-term preservation functionality in mind. The service provider has informed the Federation that data and documents older than seven years will be routinely deleted from IFRC*jobs* by the service provider.

d. *Are there procedures to ensure file integrity during transfer of your data and out of the system (e.g., checksums)?*

Yes. Security procedures have been specified in both the cloud request form (which is not a contractual document, but a document used to select service provider) and the SLA, e.g., encrypted access.

e. *Is there an explanation provided about how the service will evolve over time (i.e., migration and/or emulation activities)?*

Yes. The maintenance of both the solution and the hosting platform has been described in SLA. Depending on its frequency, maintenance can be divided into monthly patches, emergency patches, and planned maintenance (releases). Depending on its content, maintenance can be divided into adding new functionalities or modifying existing functionalities.

f. *Does the system provide access to audit trails concerning activities related to evolution of the service?*

Yes. A standard quarterly review of corrective patches and releases can be provided to the customer upon written request. Any additional service reports will be provided as an optional service, available on demand, upon payment of an additional fee.

g. *Will you be notified by the Provider of changes made to your data due to evolution of the service?*

Contract not clear. Regardless of the types of maintenance, the customer will be notified and consulted, mostly via the Release Notes Document, before the actual deployment of the release. The Release Notes will provide detailed information about the features and functionality to be delivered in the release. Some of these releases may impact the current configuration of the solution (e.g., releases); some may not (e.g., monthly patches). However, except monthly patches, in which it is stated that all existing setup and data will remain unchanged, there is no information if there will be any impact on customer's data in the other types of maintenance.

h. *Can you request notification of impending changes to the system related to evolution of the service that could impact your data?*

Contract not clear. Customer will be notified of all types of changes made to the system, but it is not clear whether impact on data is part of the notification content or not.

(5) Data retention and disposition

a. *Will your data (and all their copies) be destroyed in compliance with your data retention and disposition schedules?*

Yes. The existing Federation retention and disposition schedule for paper recruitment records is no longer applicable for records created using IFRC*jobs* (See section 7.3), but in the cloud request form (which is not a contractual document, but a document used to select service provider), the service provider did indicate that the solution allows "configuring data retention periods for candidate personal data according to local legislation". Moreover, in case the solution is used in different countries with different legal requirements, "country specific data retention periods can be applied".

b. *If so, will they be immediately and permanently destroyed in a manner that prevents their reconstruction, according to a secure destruction policy ensuring confidentiality of the data until their complete deletion?*

Yes and No. Data can be permanently destroyed, but not immediately. The hosting platform is compliant with ISO 27001 on secure disposal. However, as data backups are performed on a data center level rather than per client, backups will not be overwritten until six months later.

c. *Are you aware of the nature and content of the associated metadata generated by the system?*

Not applicable. This is a Checklist item that measures the customer's awareness on metadata. It should be investigated by asking the customer. It is unlikely that it will appear in a contract.

d. *Will the Provider destroy associated metadata upon disposition of your data?*

Contract not clear. There is no distinction between data and metadata in the contract.

e. *Will the Provider deliver and/or give access to audit trails of the destruction activity?*

No. There is no clause regarding this.

f. *Will the Provider supply an attestation, report, or statement of deletion (if required by your internal or legal destruction policies)?*

No. There is no clause regarding this.

(6) Security, Confidentiality, and Privacy

Security

a. *Does the system prevent unauthorized access, use, alteration, or destruction of your data through technical, physical, and organization measures?*

Yes. The SLA specifies the appropriate technical, physical, and organizational measures the service provider takes to protect data against unauthorized disclosure or access, accidental loss or destruction.

b. *Is your data secure during procedures of transfer into and out of the system?*

Yes. Security procedures have been specified in both the cloud request form and the SLA, e.g., encrypted access.

c. *Does the system provide and give you access to audit trails, metadata, and/or access logs to demonstrate security measures?*

No. There is no clause on this.

d. *Will you be notified in the case of a security breach or system malfunction?*

Yes. T and C specifies that the service provider shall notify the customer of any unauthorized access to Customer data without due delay. SLA states, "In the event of a data security breach, the Company will endeavor to notify the Customer as soon as the Company is made aware."

Confidentiality

e. *Does the Provider have a confidentiality policy in regards to its employees, partners, and subcontractors?*

Contract not clear. It is hard to know from the contract whether the service provider has a confidentiality policy. But T and C stipulates that the service provider and all individuals assigned by it to perform services shall "assure compliance with all applicable laws of the country where the service provider is registered as well as those in which the activities are performed", and shall not communicate at any time to any other person external to the customer any information known to it/them by virtue of its/their association with the customer.

Privacy

f. *Are there privacy, confidentiality, or security policies for sensitive, confidential, personal or other special kinds of data you store with the Provider?*

Checklist item is ambiguous. What does this checklist item mean? Does it mean privacy, confidentiality, or security policies in the customer's organization, the provider's organization, or the contract?

g. *Does the system prevent unauthorized access, use, alteration, or destruction of your personal information through technical, physical, and organizational measures?*

Yes. The SLA specifies the appropriate technical, physical, and organizational measures the service provider takes to protect data against unauthorized disclosure or access, accidental loss or destruction.

h. *Is it clearly stated what personal information is collected and why it is collected?*
i. *Is it clearly stated how the personal information collected will be used?*
j. *Does the Provider share your personal information with other companies, organizations, or individuals without your consent?*
k. *Does the Provider clearly stated the legal reasons it which they would share your personal information with other companies, organizations, or individuals?*
l. *If the Provider shares your personal information with their affiliates for processing reasons, is this done in compliance with a privacy, confidentiality, or security policy?*

Not applicable. These Checklist items appear to be written with free cloud computing services for individuals in mind and therefore are not applicable to IFRC*jobs*. The personal information stored in IFRC*jobs* is applicants' information, which is key to IFRC*jobs*'s function. The types of information collected are determined in advance.

Accreditation and Auditing

m. *Is the Provider accredited with a third party certification program?*

Yes. According to the Cloud Request Form, the service provider's platform is certified against ISO 27001 and BS 25999 standard for Business Continuity.

n. *Is the Provider audited on a systematic, regular, and independent basis by a third-party in order to demonstrate compliance with security, confidentiality, and privacy policies?*

Contract not clear. There is no clause on audit process.

o. *Is such a certification or audit process documented?*

Contract not clear. There is no clause on such information.

p. *Do you have access to information such as the certifying or audit body and the expiration date of the certification?*

Contract not clear. There is no clause on such information.

(7) Data location and Cross-border data flows

Data location

a. *Do you know where your data and their copies are located while stored in the cloud service?*

Yes. The primary and secondary data centers and their locations have been specified in the T and C.

b. *Does it comply with the location requirements that might be imposed on your organization's data by law, especially by applicable privacy law?*

Not applicable.

c. *Do you have the option to specify the location, in which your data and their copies will be stored?*

The primary data center and secondary data center are pre-determined. The Federation cannot change this, but the Federation will be provided 30 days' notice if the service provider wants to change the data centers.

Cross-border data flow

d. *Will you be notified if the data location is moved outside your jurisdiction?*

Yes. According to T and C, the service provider shall notify the customer in writing ten business days prior to any transfer of data from the hosting location and the service provider warrants that there shall be no export of customer data outside the EEA area. In addition, according to SLA, the service provider can "change the data centers within EEA during the term, provided that any new hosting centre provides at least the same level of services and security as the current data centres and will provide 30 days' notice in this event".

e. *Is the issue of your stored data being subject to disclosure orders by national or foreign security authorities addressed?*

Yes. According to T and C, the service provider shall immediately notify the customer of any seizure of data by any relevant authorities. And if either party receives a disclosure request, it shall consult the other party on how to respond.

f. *Does the Provider clearly state the legal jurisdiction in which the agreement will be enforced and potential disputes will be resolved?*

Yes. Dispute resolution procedure, and the governing law of the agreement and any dispute are specified in the T and C.

(8) End of service – contract termination

a. *In the event that the Provider terminates the service, will you be notified?*

Yes. There is a list of circumstances in which the service provider may terminate the services, but normally a prior notification will be sent to the customer.

b. *Is there an established procedure for contacting the Provider if you wish to terminate the contract?*

Contract not clear. There is information on how to contact the provider, but no information in the contract on procedure to terminate the contract.

c. *If the contract is terminated, will your data be transferred to you in a usable and interoperable format?*

Yes. According to the SLA, the data will by default be returned in either CSV or XML format, free of charge, and it can be returned in other formats by paying additional fees.

d. *Is the procedure, cost, and time period for returning your data at the end of the contract clearly stated?*

Yes. According to the SLA, the data will be returned in CSV or XML format free of charge, if written request is made within certain time. If the written request is made after the defined time length, or for other formats, then the service provider can charge for such services.

e. *At the end of the contract, do you have the right to access the associated metadata generated by the system?*

Contract not clear. There is no such information on metadata.

f. *At the end of the contract and after complete acknowledgement of restitution of your data, will your data and associated metadata be immediately and permanently destroyed, in a manner that prevents their reconstruction?*

The data will be destroyed permanently, but not immediately (see 5b.).

5.1.2 Discussions and Recommendations

Overall, the IFRC*jobs* contract is very strong with approximately 30 out of 60 Checklist items answered "Yes".

Among those items not answered "Yes", some of them are not applicable to IFRC*jobs*, as these questions are directed towards free services for individuals. Metadata related questions are consistently answered "No" as there are no specific clauses on metadata. Some checklist items are concerned with the assessment process and are unlikely to be found in a contract. Other items are concerned with the results that customer can achieve by using the service, which the provider is unlikely to guarantee. A more detailed discussion of the results follows.

(i) It is stated at the beginning of the Checklist that, "The target audience for this document is records managers and archivists assessing cloud services for their organization and/or institution." This purpose statement is slightly at odds with the title of the Checklist, which is focused on "Cloud Contracts" per se. Perhaps due to this ambiguity, while the majority of the items in the checklist are about components of the contract, a few items are questions that customer can ask when conducting a risk assessment, e.g., (5)c, 7(b), and 7(c), prior to the procurement of the service.

(ii) Some of the items in the checklist are based on the assumption that the cloud service is a free service to individuals which generates revenue by selling personal data collected from the individuals, e.g., (2)c, (6)g, (6)h, (6)i, (6)j,(6)k,(6)l. However, IFRC*jobs* is a cloud-based service to an organization that pays to use the service. Therefore, the Checklist items referred to above are not applicable to IFRC*jobs* nor to other cloud computing services provided to and paid for by organizations.

(iii) Some items are repeated one or more times under different issues. For instance, both (5)b and (8)f are about the manner in which data will be destroyed regardless of whether this destruction is triggered by the retention and disposition schedule or the end of services; both (6)a and (6)g are about the technical, physical, and organizational measures implemented to prevent unauthorized access, use, alteration, or destruction of data, regardless of whether it is business data[1] or personal information; both (4)d and (6)b are about the integrity of data at rest and in transit.

(iv) Some items are concerned with the impact of using cloud-based service on freedom of information ((3)c), availability of data ((3)b), e-discovery ((3)e), and access to information ((3)d). These are results that customers can achieve from using the service. These should be assessed by the customer based on the data about the service. It is unlikely that the service provider will provide such guarantees in a contract. These issues should be approached from a risk management perspective wherein customers have to

[1] In IFRC*jobs*, the business data includes personal information about job applicants, which is not to be confused with personal data of individuals who contract a cloud computing service.

[2] http://www.pre.ethics.gc.ca/eng/policy-politique/initiatives/tcps2-eptc2/chapter3-chapitre3/#toc03-1d

assess potential risks based on the service's availability and other features. They can then either seek to mitigate or accept the potential risks.

(v) Some information, though important (e.g., (6)m,n,o,p), is unlikely to be included in a contract. For instance, the customer can ask the provider to provide its accreditation information and process as part of the pre-selection evaluation of the service provider, but this may not be directly relevant for inclusion in the binding contract between the provider and the customer.

(vi) Records management issues, particularly the generation, storage, access, and destruction of metadata, are consistently missing from the IFRC*jobs* contract. Interviews with relevant staff indicate that they believe there is no need to distinguish between data and metadata; metadata is one kind of data and will be addressed by clauses on data. This is one major weakness of IFRC*jobs* contract. Given the crucial role metadata plays in the creation, maintenance, and long-term preservation of records, it is vital that the Federation pay heed to metadata issues in future cloud service contracts.

5.2 Contract Analysis Using the Retention & Disposition Functional Requirements

5.2.1 Analysis Results

Privacy and Security Considerations

(1) Does the vendor allow independent audits of systems and processes?

Don't know. Though staff from the Risk and Audit department (interviewee) maintained that when negotiating a contract with the service provider, they always make sure that there is a clause that gives the Federation the right to audit, our examination of the contract did not identify any such clause or any clause to that effect. In addition, since the introduction of the IFRC*jobs* is very recent, the Federation has not yet conducted any audit of the application. Yet, interviewee 6 did confirm that because of the specialized IT knowledge required to audit the service provider, they would have to outsource the audit to external companies.

(2) Is the content encrypted when in transit to the cloud?

Yes.

(3) Is the content encrypted when at rest in the cloud?

Yes.

(4) Are the physical servers located within a jurisdiction approved for your organization?

Not applicable. This item is formulated with the assumption that the jurisdictions where the organization's physical servers are located have to be approved by a/an oversight/governing/regulatory organization. This premise is not applicable to the Federation, which is an international organization that enjoys privileges and immunity in Switzerland and in countries that sign status agreement with it.

One suggestion is to refine the preposition used in the Checklist item to accommodate special organizations like international organizations, for instance, *are the physical servers located within a jurisdiction approved for* ***and/or by*** *your organization?*

(5) Are the backup servers located within a jurisdiction approved for your organization?

Not applicable. Same as above.

Establishing disposition authorities

(6) What indexing capability is supported (can it accommodate customers' taxonomy for indexing)?

Don't know. These are two questions. The answers to both questions would be "Don't' know". As to the indexing capability of IFRC*jobs*, to the best knowledge of the researchers, no special indexing function is provided. The application is designed in such a way that records related to the recruitment process, the candidates, the job opening, and other recruitment subject could be viewed.

Since IFRC*jobs* is only used for recruitment and only one category of records is generated, no taxonomy for indexing (or classification schedule) is applied in IFRC*jobs*.

When reading this Checklist item, the researchers were a little bit confused over the use of "customers" in this item. Does it refer to the Federation, namely the service provider's customer, or the Federation's customers? One suggestion is to change "customers' taxonomy" to "your organization's taxonomy" to be consistent with the rest of Requirements. Otherwise, it is likely to cause confusion.

(7) Can retention periods be applied?

Yes. IFRC*jobs* is used to support one specific function within the Federation—recruitment. According to the Federation's retention and disposition schedule, recruitment records are grouped into one category and are, therefore, all subject to the same retention period. Theoretically, the retention period should be able to be applied to the records. The issue centers on the applicability of the original paper-based retention periods to electronic records (See section 7.2).

(8) Can destruction be automated?

Don’t know. Due to the uncertainty over the applicability of original retention and disposition schedule, recruitment records generated by IFRC*jobs* are to be preserved for seven years—the maximum length of time allowed by the service provider for free (See section 7.2). The Federation has only two years’ experience with IFRC*jobs*, so no destruction has been performed so far. Therefore, it is not clear whether destruction can be activated automatically, or requires human intervention.

Applying disposition authorities

(9) Can a disposition authority (retention and disposition specifications) be applied to aggregations of records?

Yes. Records generated by IFRC*jobs* are recruitment records and belong to the same category. Retention and disposition specifications can be applied to the aggregations of recruitment records.

(10) Can records be locked down for viewing only?

Yes. In a different context—for security reasons in this case—interviewees confirmed that users might only be able to view certain records, or not view certain records in some cases, based on their access right. Therefore, it is inferred that records should be able to be locked down for viewing only, for whatever purpose.

(11) Can records be retained indefinitely?

Don’t know. This item can be interpreted in many ways, and therefore, be answered in different ways. First, if this question intends to assess the capability of the application to retain records indefinitely, there is no reason to doubt why this cannot be done. Second, if this question intends to assess whether the service provider allows the records be retained indefinitely, currently the service provider allows records to be retained for a maximum of seven years for free. However, as long as the Federation is willing to pay the storage fee, the records should be able to be retained for as long as the Federation requires. Third, if this question intends to assess the long-term preservation ability of IFRC*jobs*, the application is not expected nor intended to fulfill such a function.

(12) Can records not in an aggregation be destroyed at a future date?

Yes.

(13) Can records not in an aggregation be transferred at a future data?

Yes.

Executing disposition authorities

(14) Can records be deleted according to the retention/disposition schedule?

Yes.

(15) Can backups be deleted according to the retention/disposition schedule?

Yes. But because backups are performed at data center level rather than per client, backups cannot be over written until the next backup cycle, which occurs every six months.

(16) Are users alerted to conflicts related to links from records to be deleted to other records aggregations that have different records disposition requirements?

Don't know. Due to the uncertainty over the applicability of the retention and disposition schedule, thus far, it has not yet been applied to records generated by IFRC*jobs*.

(17) If more than one disposal authority is associated with an aggregation of records, can these multiple retention requirements be tracked to allow the manual or automatic lock or freeze on the process (ex. Freeze for litigation or freedom of information request)?

Yes. Freezing disposal authority/action is a manual process.

Documenting disposal actions

(18) Are disposal actions documented in process metadata?

Yes and no. Archiving of job postings and of candidate profiles is documented. Deletion of candidate profiles is partially documented. Deletion of job postings is not documented.

(19) Can all disposal actions be automatically recorded and reported to the administrator?

There are two questions embedded in this item. The first question asks whether all disposal actions can be automatically recorded, which is a repeat of item #18. As to the second question, disposal actions are not automatically reported to the administrator.

Reviewing disposition

(20) Are electronic aggregations presented for review along with their records management metadata and disposal authority information so both content and records management metadata can be reviewed?

Yes.

(21) Can records be marked for destruction, transfer, further review?

Yes.

(22) Are all decisions made during review stored in metadata?

No.

(23) Can the system generate reports on the disposition process?

Yes, for archived job postings and candidate profiles, and for deleted candidate profiles.

(24) Is the ability to interface with workflow facility to support scheduling, review, and export transfer processes provided or supported?

Don't know.

Integration

(25) Is the metadata schema compatible with other systems, such as Enterprise Content Management or Records Management Systems?

Don't' know. The Records Management System has been introduced very recently, and no attempt has yet been made to map the metadata of IFCRjobs against the metadata of the Records Management System. Staff involved in the evaluation and introduction of IFRC*jobs* revealed that inadequate attention was given to metadata when evaluating and introducing IFRCjobs.

5.2.2 Discussions and Recommendations

Overall, this analysis shows that some of the items in the Retention & Disposition Functional Requirements work well, but some do not. Among the 25 items, ten are answered "Yes"; twelve are answered "Don't know"; two are answered "Not applicable".

The major issue we identified is that assumptions on which these Functional Requirements are based may not be applicable to an organization that uses the Requirements. For instance, it is assumed that the cloud service will serve as a records management system that manages all records generated by the organization and is able to apply a classification plan (#6) and retention and disposition schedule (# 9~24). But the organization may only expect a cloud service fulfill a business function and not serve as a record keeping or records management system. Further, it is assumed that the organization should abide by regional, national, or industry regulations; hence, the geographical locations where the physical servers of the service provider are located should be approved by such governing organizations. But for international organizations like the Federation, this is not applicable. In addition, it is assumed that a neat, standardized digital records management program is established in the organization. But the records management reality is usually complex, involving a hybrid of different records management systems (e.g., paper, business computer applications that serve as de facto records management systems, and an electronic records management system).

The following is a list of recommendations we would like to make to aid the improvement of the Retention & Disposition Functional Requirements.

(i) For item #4, we recommend to refine the preposition used in the item to accommodate special organizations like international organizations, for instance, *are the physical servers located within a jurisdiction approved for* ***and/or by*** *your organization?*

(ii) For item #6, there are two questions embedded in this item, we recommend splitting it into two questions.

(iii) For item #6, when reading this item, the researchers were a little bit confused over the use of “customers” in this item. Does it refer to the Federation, namely the service provider’s customer, or the Federation’s customer? One suggestion is to change “customers’ taxonomy” to “your organization’s taxonomy” to be consistent with the rest of Requirements. Otherwise, it is likely to cause confusion.

(iv) For item #19, there are two questions embedded in this item. The first one is a repeat of item # 18. We recommend removing the first one and only keeping the second one.

(v) Considering the issue we identified in section 7. 2, we suggest that the researcher take into account any influence the use of cloud-based services may have on the applicability of the original retention and disposition schedule.

(vi) This Functional Requirement is based on the assumption that the cloud service to be examined will serve as a single records management system to manage all the records generated by the organization. However, this may not always be the case. As in this case, the cloud service to be examined may only function as a recordkeeping system for the category of records generated by itself. We advise that the researchers re-examine this assumption.

(vii) Another assumption on which this Functional Requirement is based is that the organization has a well-established and uniform digital records management program. Again, this may not always be the case. As in this case, the organization may have a hybrid records management program comprising paper records management system, and digital records management system. We advise that the researchers re-examine this assumption.

6. System analysis

Formally launched on 7 January 2014, the aim of IFRC*jobs* is to streamline, standardize, and improve the recruitment process, and transform the recruitment process from being paper-based to being conducted electronically. When communicating the introduction of IFRC*jobs* to the staff at the Federation, the following features of IFRC*jobs* were highlighted: electronic validation, recruiting all categories of staff, visibility, user-friendliness, dashboard/reporting, efficiency, and flexibility.

The recruitment process embedded in IFRC*jobs* is comprised of the following steps: creating a job opening by the hiring manager; approving the job opening by HR, the finance department, and the second line manager; posting the job on internal and/or external websites; screening applicants; matching candidates to open positions; selecting candidates; and hiring candidates. Depending on the job opening, the step of selecting candidates further involves the following steps: technical review; interview; reference check; and background check. The detailed recruitment process can be defined and configured by the administrator of IFRC*jobs* based on the business rules of the Federation.

Extensive and sufficient documentation capability has been integrated within IFRC*jobs*. Each action performed using IFRC*jobs*, including time of the action, author of the action, content of the action, sender, and recipient, is recorded. In general, the information is organized along two dimensions: the job and the candidate. For instance, users with rights have an overview of the job description, its status, and its recruitment process (including the related actions taken in each step of the process). Similarly, users with rights have an overview of each candidate, the jobs for which the candidate applied (including the selection steps), the documents the candidate uploaded (e.g., CVs, contact information, candidate summary) and documents generated by the system. IFRC*jobs* logs a history of all the actions related to the candidate, including time of the action, the specific job the action is performed on, and the author of the action. In addition, IFRC*jobs* has integrated communication within the system: users can contact candidates, notify recruiters, and schedule interviews through system-generated emails and calendaring rather than use separate communication methods. This centralizes the records of recruitment-related written communications within IFRC*jobs*.

The sophisticated documentation capability and communication ability, along with the way the information is organized and displayed ensures that the recruitment process is documented in a detailed, impartial, and transparent manner. With these records, the recruitment process can be reconstructed in the future if such needs arise. As interview 10 commented,

> *[B]ecause the different steps involved, from pre-selection to shortlist, and then the interviews, and after interviews, panel members record their feedback. ... So in terms of that, I think it is really good, because one can always go back to that and see, ... how an assessment was made. I think for transparency, audit purpose, it helps us show that the process is transparent, the decision was made based on a fair grading system for all candidates.*

7. Management of Records Created Using SaaS Applications

7.1 A Hybrid Records Management System

Once records are created, recordkeeping processes have to be performed on records to ensure records can be managed to serve the organization's current and future business needs, support the organization's accountability, and maintain transparency. The *ICA Principle and Functional Requirements for Records in Electronic Environments -Module 3* identifies three options for implementing records management functional requirements, including:

- designing the business system to internally perform the records management functions;
- integrating with an identified records management system, such as an electronic records management system; or
- designing export functionality into the business systems to directly export records and their associated metadata to an identified records management system.

The decision as to which approach to adopt for a particular business system is influenced by a number of factors, such as business needs, the overarching records management framework, technical feasibility, and regulatory requirements (ICA 2008).

This decision process remains relevant to the management of records created by SaaS applications. Moreover, the technical infrastructure of a SaaS application, which is deployed and maintained by the service provider and is highly standardized with limited customization ability, suggests that this decision has to be made early and that the corresponding recordkeeping functional requirements be incorporated into the non-functional requirements used for evaluating and procuring the SaaS application.

At the Federation, records management is not systematically and consistently considered in the adoption of cloud-based services, nor, for that matter, when applications are installed on in-house servers. The records manager has been invited to contribute to the specification of functional requirements of some systems to be procured, but in other cases records management concerns were only considered after a system had been implemented.

In accordance with the ICA requirements, when offering advice, the first issue the records manager addresses is what approach to adopt to manage the records created by the SaaS application to be procured: is the SaaS application going to perform records management functions internally, be integrated with an external records system, export records to an external records system, or print out the records. Each approach has different requirements for the underlying technical infrastructure. For instance, if a SaaS application is going to internally perform records management functions, then it must be able to apply retention and disposition schedule, document related metadata, ensure the integrity of the records, and transfer records of permanent value to archives. Applications have to be examined on a case-by-case basis. For instance, for one specific system (i.e., e-travel system) at the Federation, despite the system having comprehensive capabilities for records management, recordkeeping has to be done outside the system on paper for audit reasons. As a result, records generated by the system and required by auditors have to be printed out and managed in paper format. Yet, for another system (i.e., contract lifecycle management system), which is considered as a recordkeeping system, not only are all the records generated by the system to account for the conduct of business in the system appropriately managed by the system, but also records generated in paper format are scanned and uploaded into the system.

In the case of IFRC*jobs*, unfortunately, recordkeeping was not considered in the functional requirements phase. The foregoing system analysis shows that IFRC*jobs* is able to document adequately the business activities and transactions embedded in the recruitment function, thereby, generating records. However, the management of these records may not be without problems. For instance, metadata, which is crucial to identify, authenticate, contextualize, and manage records, is defined without adequate concern to records management. When Interviewee 3 (staff from the legal department) and Interviewee 4 (staff from the IT department) were asked to talk about how metadata issues were addressed in contract negotiation, they indicated that they did not apply that "level of scrutiny". When implementing the application, the service provider sent IFRC a massive spreadsheet for it to configure the application based on their needs, such as email address, the list of default countries appear on the drop down. Yet, it appears that records management was not a criterion considered when making such configuration.

At present, records created by IFRC*jobs* are managed in a hybrid manner. The entire record of a recruitment is retained in the application, hence, in the cloud, although no classification scheme and retention and disposition schedule are applied to the records. When the recruitment process is completed, copies of certain documents created in or loaded into IFRC*jobs*, namely the Request for Staff and the successful candidate's CV must also be filed in the electronic personnel file of the individual hired to fill a vacant position. This personnel file is kept in the Federation's newly installed Records Management System.

7.2 Retention and Disposition: Beyond Compliance

The existing retention and disposition schedule developed for paper recruitment records at the Federation indicates that, except for certain records that are required for long term preservation (e.g., successful candidates' CV), recruitment records will be kept for two years and then destroyed. The two-year retention period is primarily determined by the audit cycle, the time during which applicants can raise questions or file complaints about the recruitment process, information usage requirements for current business needs, and the archival value of recruitment records. Among these factors, the time during which applicants can contest the recruitment process, for instance disputing that there is favoritism to somebody, or the process is flawed, is the dominant factor. In regard to other factors, use of recruitment records in paper format for current business needs is quite limited, because it is very troublesome to identify and reuse any information in paper recruitment records. In addition, storage and maintenance of paper recruitment records requires significant resources. Due to this cost/benefit imbalance and the audit requirement for the minimum retention period of recruitment records, the Federation set the retention period of these paper records to the minimum two years and destroyed them after two years.

With the use of IFRC*jobs*, while the two-year period for contest and audit cycle remains valid, the switch from paper format to digital format has considerable impact on other factors influencing the retention period. First, compared to paper records, it is more convenient to reuse recruitment records for purposes (e.g., strategic and operational purposes) not envisaged for paper records. Moreover, most SaaS applications, including IFRC*jobs*, now provide some extent of data analysis functionality such as generating report and analytics, which facilitates data reuse. Second, currently, IFRC*jobs* service is purchased based on transaction rather than storage. Storage in IFRC*jobs* of data about a particular transaction is free for a maximum of seven years, which is much longer than the two-year retention period. These two factors have reversed the imbalance between cost and benefits such that there is zero cost for huge potential business benefits. This creates a situation wherein, on the one hand, there are organizational regulatory requirements stipulating that recruitment records be kept for at least two years for audit purpose; on the other hand, free storage and potential business benefits prompt the Federation to keep records longer. Since the records manager was not involved in the evaluation and introduction of IFRC*jobs*, this conflict was not considered from the beginning. At the moment, the retention and disposition schedule for recruitment records is not followed; and recruitment records generated and received by IFRC*jobs* will be kept for seven years. Nonetheless, this is simply a temporary adjustment in light of the changes brought about by the use of cloud-based services, and is in no way to be considered a final long term solution. Additionally, the seven-year retention period may not be completely beneficial for the reuse of recruitment records, as some data may be too old and it adds additional cost to searching through unweeded data. Interviewees commonly noted that the use of cloud services in general, and this IFRC*jobs* application in particular was still new at the Federation and more experience is needed before they could appropriately address these issues.

At the present, records management work is primarily advocated and performed in an accountability-based approach. Records are considered as evidence that organizations can use to reconstruct their decision-making process, therefore, discharging their accountability to their "clients". This approach is comprised of an integrated set of theories and methodologies ranging from the definition of records, to justifiable retention and disposition of records. It can be identified as compliance-based wherein legal compliance is the dominant criterion, if not the only one, in guiding decisions for records management. However, with the extensive storage capacity and the massive opportunities to exploit data for strategic and operational purposes offered by the cloud and other new technologies, it is hardly surprising that more and more organizations start incorporating potential business value of records management into the set of principles guiding records management decisions. This indicates that records management may go beyond legal compliance to take multiple values of records into consideration when designing and performing records management.

7.3 Long-term Preservation of Records: in Paper Format

The Federation has its own internal archives in which records of long-term preservation value will be deposited. At present, the Federation primarily relies on paper format for permanent preservation of records; therefore, records that will be transferred into archives have to be printed out. Interviewee 9 explained that electronic systems at the Federation did not have the capacity for the long-term preservation of records, and there was also "no intent right now of building a digital archives". Although the Federation tries to keep records in digital format as long as possible (for the sake of current business needs), they don't have confidence in using digital format for long-term preservation.

As more and more analog business functions and processes are transformed into digital ones, or moved into the cloud, the continuing use of paper format for long-term preservation creates another divide in the Federation's records management in addition to the hybrid records management system. This raises some new issues, for instance, how to determine the "cut-off point" where it is no longer necessary to keep records in digital format for the purpose of current business needs, and the increasing difficulty of implementing records management policies across different business systems, recordkeeping systems, and across different formats.

7.4 Data Security and Privacy Protection

Existing research shows that data security and privacy protection is often cited as one of the major factors inhibiting organizations from using cloud-based services. This is also one of the major risks considered by the Federation when evaluating and introducing cloud-based services. To effectively address this risk, an integral set of mitigation strategies and solutions has been put in place, ranging from cloud strategy, to due diligence in evaluating and selecting cloud service provider.

Cloud Strategy

As discussed above in section 4.1, the introduction of cloud-based services is primarily a process of balancing the risks and benefits of different adoption options; and one of the key parameters in assessing the risks and benefits of each adoption option is data security and privacy. When asked how the Federation addresses the risks related to the use of cloud-based services, interviewees frequently highlighted "classification of data", "the type of data", or "information classification standard". As discussed above in section 4.1, all these refer to the Federation's information security classification framework, which classifies information into four categories according to their sensitivity level and the possible consequences the Federation may face if the information is not appropriately protected. These four categories are highly restricted, restricted, internal, and public. Highly restricted information and restricted information are often mentioned by interviewees as well, as these two categories of information are the ones the improper handling of which will result in significant impact on the Federation. In addition, despite not being explicitly mentioned in the information security classification framework, it seems that once personal information is being collected, processed, or stored by a business process or function, the information and/or records generated will mostly be categorized as highly restricted or restricted information. This arises from the concern over privacy protection. Thus, data privacy, along with data security, is being addressed from the very beginning.

Once the information involved in the business process and functions to be migrated to the cloud has been categorized according to the information security classification standard, the result can help guide the selection of the most appropriate technology service provision model: on premise software, private cloud service, or public cloud service. The risk levels of these three options from high to low are public cloud service, private cloud service, and on premise software. Considering the level of care required and the possible consequence of mishandling, highly restricted information and restricted information would preferably be managed using on premise software, or private cloud service. Therefore, when initially defining the cloud strategy, the Federation considered using "pure private cloud" for all their applications. However, this will involve immense cost, which will offset the benefits of using cloud-based services. To leverage the benefits of cloud-based services and, yet, to best comply with information security classification standard, the Federation determined that extremely critical applications (e.g., financial applications) will be migrated to private cloud, and less critical ones will be migrated to public cloud.

The collection and storage of personal information in the recruitment process escalates the security level required to that of highly restricted information or restricted information. However, due to a variety of other factors (e.g., availability, and quality of recruitment computer applications in private cloud), the Federation chose a recruitment computer application based on public cloud. This poses a challenge to successfully complying with the information security classification standard.

Due Diligence in Evaluating and Selecting Cloud Service Provider

Due to the potential risks associated with the use of public cloud based application for recruitment, the Federation exercised due diligence in evaluating and selecting the service provider.

Geographical location

The geographical location where the service provider is based, and where its servers are located has significant legal implications, as this indicates to which jurisdiction's legislation the Federation's data is subjected. In the case of the Federation, despite being an international organization, it only enjoys inviolability of archives in Switzerland and in countries with which it signs a status agreement. This makes the risks associated with cloud-based services all relevant to the Federation. In fact, our interviewees acknowledged that they did not treat themselves special—relying on their status as an international organization to save them from any potential risks associated with the use of cloud-based services—when evaluating and assessing cloud service providers.

As discussed in section 4.1, preferably, the Federation will choose service providers, first, in Switzerland (considering that the Federation enjoys inviolability of archives in Switzerland), second, in Europe (considering that privacy legislations in Europe are more stringent than in other countries). In light of the stringent legislations in Europe, selecting cloud services in Europe gives the Federation more time to intervene and to gain the initiative in certain situations. The Federation has serious concerns about service providers from the United States because of its legislation. However, this does not mean that they are "averse completely to using American companies"; rather, it means that they will use American companies for less critical information or for only certain types of cloud deployment models (e.g., private cloud).

In the case of IFRC*jobs*, both the service provider, and its servers (the major data center and the backup data center) are in Europe. The Federation also negotiated that "any new hosting centre provides at least the same level of services and security as the current data centres and will provide 30 days' notice in this event" (SLA Sec.6).

Technological examination

In addition to restrictions placed on the geographical locations of the data center, the Federation also conducted a comprehensive examination of the technological capabilities of the service provider to determine its ability in protecting data security and privacy.

In the initial screening of service providers using the Cloud Request Form, the Federation investigates whether there is a risk that the service provider may wrongfully delete or access data, whether there is a risk that the Federation's data will not be properly removed from the cloud network infrastructure upon termination of cloud services, and whether there is a risk of the Federation's data being compromised while it is in transit or at rest. For each question, the service provider provides detailed information about how system backup is conducted, how disaster recovery is performed, how data will be returned upon the termination of cloud service, how data and its backup will be deleted, and the encryption measures.

Further, in the Service Level Agreement, availability of the service and response time (including the definitions and service credits) have been defined. The security infrastructure at the service provider's data center, including physical security, data center environment, data center network, data center network, security applications installed at the servers, system backup, and disaster recovery procedures have also been specified at the Service Level Agreement.

Standards

Another important parameter the Federation used in ascertaining the security level of the service is the use of standards. For instance, interviewees highlighted the standards used for pricing, standards used for the integration between the cloud service and the Federation's database or web portal, types of standards the service provider's services support, and standards used in other parts of the service. The Federation prefers that the service provider use well-known and stronger standards, which usually indicates higher level of security.

Notification

Other than proactive measures, the Federation negotiates that the service provider sends the Federation prior or immediate notification in case of a series of events so that the Federation can gain initiative and positively intervene to resolve issues ensuring that the Federation can avoid or mitigate any potential risks.

Events that require prior or immediate notification include termination of agreement due to material breach of any term in the Terms and Conditions (T and C 4.3), termination of agreement due to any use of the solution not in accordance with the Agreement (T and C 4.4), increase of fees (T and C 6.1), suspension of the provision of service due to late payment (T and C 7.3), "any wrongful deletion of Customer data or of any seizure of data by any relevant authorities" (T and C 8.7), "any unauthorized access to Customer data" (T and C 8.8), and "any transfer of data from the hosting locations" (T and C 8.9). All the notices required "shall be in writing and shall be deemed to have been duly given if sent by registered post or acknowledged fax to a party at the address given for that party in the Order Form" (T and C 21).

7.5 Other issues

Destruction of data

The service provider is ISO 27001 certified in terms of the methods used for the deletion of data. It is specified that the Federation's data shall be destroyed 3 months from the termination of the contract at the latest. It is also stated in the Terms and Conditions that data in the primary data center shall be deleted 30 days after the termination of the contract but that, since data backups are made on a data center level rather than per client, backups cannot be overwritten until the next backup cycle, which usually is six months later (T and C 8.6).

Ownership of data

The clause that directly addresses the issue of ownership of data only focuses on the ownership of personal data. It is stated that "To the extent that personal data is processed" using the application, the service provider is a "data processor" and the Federation is a data controller; the service provider "will only process personal data on behalf of, and in the name of, the [Federation]" (T and C 8.2).

Third party access to the Federation's data

In the Terms and Conditions, the service provider warrants that "no other third party than subcontractors shall have direct access to" the Federation's data (T and C 9.7). Meanwhile, the service provider shall notify the Federation of any unauthorized access to the Federation's data (T and C 8.8).

Disclosure request

The Terms and Conditions has specified that, if either the service provider or the Federation receives a disclosure request, such party shall "(i) promptly consult with and take into account any comments from the other party prior to making any disclosure; and (ii) work with the other party to ensure that any exemptions or other legitimate means of preventing disclosure or limiting disclosure are used to the fullest extent possible" (T and C 12.5).

8. Partnership

Despite all the due diligence conducted in evaluating and selecting service providers, and the efforts made in negotiating a contract that is in the Federation's best interests, or at least that is fair and protective to both parties, the nature of cloud services means that it is unlikely that the Federation can completely eliminate any potential risks.

Nature of cloud (or the tool, SaaS, or IFRC*jobs*) was frequently referred to in interviewees' discussion, suggesting that the Federation has a good understanding of the coexistence of benefits and risks in using cloud services. Indeed, it is unlikely that a service provider will warrant one hundred percent "uninterrupted or error free" service. In fact, in the Terms and Conditions, it is explicitly stated that "No warranty is made regarding the results the Customer can achieve from using the Solution and Services nor that the Solution and Services will operate uninterrupted or error free" (T and C 9.4). In addition, it can be difficult to measure or quantify the impact the Federation may experience from a failed service or to evaluate the liability the service provider should pay for a service failure. Therefore, the complete control consumers strive for in using cloud services may seem elusive. In place of the lost control is partnership, as interviewee 4 observed,

> "This is why the relationship side is more important than the contractual document. It is really working on how you make that relationship work, what you get out of them, how you shift the balance of power, what respective benefits both parties get."

Indeed, the willingness to enter a five-year contract in this case requires flexibility and cooperation from both parties to make this relationship work and to guarantee the quality of the service delivered. While the contractual documents can establish the quality of the service the service provider should deliver, it is mostly through a partnership relationship that the Federation and the service provider can work together to resolve any issues and to guarantee the service quality. For instance, immediately after IFRC*jobs* went live, there were some issues with the service provider's platform. As a result, the Federation experienced a series of incidents with IFRC*jobs*. To make matters worse, there were some issues with the communication with the support desk because of the way the ticketing system worked. An incident report would go from one level to another, in a long process to finally reach the support technician who could help resolve the issues. As interviewee 7 commented, they were not satisfied with the service at that time. The Federation discussed the issues with the service provider, who treated the issue seriously. Ever since the discussion, the communication channel between the Federation and service provider has been improved; now the Federation can contact the support technician directly without having to go through the filtering process.

9. Conclusion

Despite the advances made in recent years, the use of cloud services in organizations is still recent. Recognizing the potential of cloud services in transforming IT service, organizations now are actively exploring how to utilize this new technology and, in the meantime, protect themselves from potential risks. In the process, they continuously educate themselves about this new technology. This case study presents a good illustrative example of how an international organization understands the strategic value of cloud computing in its IT strategy and its organizational strategy and mission, how it designs the cloud strategy and roadmap, how various issues and risks associated with cloud services are addressed, how records generated by the use of cloud services are managed, and other relevant topics.

The evaluation and introduction of cloud services usually require the collaboration of multiple stakeholders, e.g., business department, IT department, legal department, and risk and audit department. Each stakeholder will contribute differently in order to guarantee the successful delivery of the cloud service. From a project management perspective, while there is no substantial difference in the introduction of a cloud-based application, the characteristics of cloud-based applications (e.g., limited ability to customize, multiple clients to serve) propel the Federation to rethink and reexamine their business processes, therefore, providing a good opportunity to reengineer their business processes.

In comparison with traditional on premise applications, cloud-based applications may be more intuitive and easy to use; they also have much more capabilities (e.g., social network capabilities, ability to communicate with higher managers and line managers). In addition, the use of cloud-based applications allows the Federation to enjoy better IT services with limited resources. The short delivery timeline also gives the Federation the luxury to test the product within days and to examine the non-functional features of the application, e.g., interface, user friendliness.

Risk management plays a central part in the Federation's introduction of cloud-based services. Another two key constructs are control and trust. Many factors have been taken into consideration in the risk management process. Some of the factors are commonly acknowledge by research studies and practitioners, such as the geographical locations where the service providers are located, where the servers are located, and where the backup servers are located, the classification of data, highly confidential information, legal compliance, standard used in the application, how mature the service providers are, and economic benefits. Some of the factors are not commonly recognized by other studies, such as how comfortable the Federation is with the service providers, or the products, and the partnership relationship between the Federation and the service provider.

Consistent with other research studies, this case study shows that records management is not adequately and consistently considered in the introduction of cloud-based services. The primary question the records manager considered when evaluating a cloud-based service is whether the service is going to serve as recordkeeping system or not, and hence, how records generated by the application are going to be managed. The complex records management environment—a hybrid of different records management systems—creates additional issue for addressing the challenges raised by the use of cloud-based services.

This case study raises more questions than answers. It has identified several areas that require further research, such as the relationship between risk management, control, and trust in the use of cloud-based services, how to address the challenges raised by cloud-based service in the complex records management environment, and how to effectively monitor cloud services, in particular, its compliance with the service level agreement.

10. References

IFRC (2012) “Mission Relevant IT: 2012 ISD Annual Report”. Available at: http://www.google.ca/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CB0QFjAA&url=http%3A%2F%2Fadore.ifrc.org%2FDownload.aspx%3FFileId%3D51162%26.pdf&ei=4oOMVbmOJ8uuogTwlr2QDg&usg=AFQjCNE4HPsz4Dn4nVRIpQZ15-7eif-U6w&sig2=3DELQCuzP7fMkHjjuiT7OA&bvm=bv.96782255,d.cGU&cad=rjt (Accessed: January 26, 2016)

IFRC (2013) “Request for Cloud Services”. Internal IFRC document.

IFRC*jobs* service provider (2013) “Cost Estimate and Order Form”. Internal IFRC document.

IFRC*jobs* service provider (2012) “Terms and Conditions”. IFRC internal document.

IFRC*jobs* service provider (2012) “Service Level Agreement”. IFRC internal document.

IFRC*jobs* service provider (No date) “User’s Guide”. IFRC internal document.

IFRC (2012) “IFRC Cloud Strategy & Roadmap”. IFRC internal document.

IFRC (2014) “Information Classification Standard”. IFRC internal document.

IFRC (2013) “IFRC ICT Security Policy”. IFRC internal document.

Appendix A: Interview Guide

Interview Protocol

Case study: IFRC*jobs*, a SaaS recruiting tool

Interviewee Identifying Information

Date:

Method of Interview: Skype/Telephone/In-person

Department:

Unique ID for the Department:

Name of the Interviewee:

Unique ID for the Interviewee:

Introduction and Consent

My name is *[name],* a PhD student at the School of Library, Archival and Information Studies at the University of British Columbia (the iSchool at UBC). I am a graduate research assistant for the InterPARES Trust project, and today I would like to ask you some questions about the IFRC*jobs*, as part of a case study being conducted for InterPARES Trust.

I have a brochure, which I would like to leave with you, that introduces InterPARES Trust in more detail. *[Pass a brochure about InterPARES Trust to the interviewee]*

The purpose of this case study is to take IFRC*jobs* as a case to examine the issues raised with the use of cloud service. The findings of this case study will be used to compare with the general findings of other InterPARES Trust research and help identify the gaps between "reality" and "standards of practices". So there will be no right or wrong answer to the question that I will ask. And don't worry if you don't know how to answer the question. But for the question you know the answer, it will more helpful if you can go into much detail.

If you have any question about InterPARES Trust or this case study, please let me know.

I will be taking notes as you talk, but I would also like to use a recorder to help with my note-taking and subsequent analysis by the InterPARES researchers. Do you mind I tape record out conversation?

[*Wait for reply*]

Can I answer any question for you at this point?

Before we progress any further with this interview, I would like to obtain your consent to participate in the interview according to Article 3.12 of *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans*[2]that UBC complies with.

I need to go over your rights and what you can expect from us as an individual participating in this research study. I would like to reassure you that your participation is completely voluntary and that you have the right to withdraw from the interview at any point. I am now going to give you a human subjects consent form that outlines what I have just gone over with you. I would like you to take a few minutes to read it over, and then, if you don't have any questions, to sign it.

[*Pass the consent form to the participant*]

[2] http://www.pre.ethics.gc.ca/eng/policy-politique/initiatives/tcps2-eptc2/chapter3-chapitre3/#toc03-1d

Interview Questions

I For Staff From Records Management Department:

1. Were you involved in the evaluation and introduction of IFRC*jobs*? If yes, in what way?
2. Did you consult any records management guidelines or checklists when conducting the evaluation? If yes, what are the resources consulted, and are they helpful? If they are not helpful, what recommendations do you have to improve such resources?
3. The previous system used for e-recruitment is called JobNet, right? It is also delivered through software as a service, right? What do you think are the differences between IFRC*jobs* and JobNet?
4. Does your organization store the information/records produced by IFRC*jobs*?
5. Does your organization manage the information/records produced by IFRC*jobs*? If yes, how do you manage them?
6. If yes, what kinds of information are considered as records? Some examples include applicants' CV, correspondence letters with applicants. Are there any new forms of records? Did you encounter any difficulty in identifying records?
7. What risks does the use of IFRC*jobs* pose to records management?
8. How will you evaluate the current contract in terms of its capability to address records related risks? Are you satisfied with the contract from the perspective of records management?
9. Do you have records/information policies for the use of IFRC*jobs*?
10. Who owns the records produced by IFRC*jobs*, your organization or the service provider?
    a. Who owns the meta-data created by IFRC*jobs*?
11. Who owns the copyright of the records produced by IFRC*jobs*?
    a. Who owns the copyright of the meta-data created by IFRC*jobs*?
12. How do you apply your organization's retention and disposition schedule to records produced by IFRC*jobs*? Did you encounter any difficulties? If yes, what are they, and how did you address them?
13. How about the retention and disposition of candidates' personal data (e.g., name, address, family information, and CV)? Will they be treated separately from other general information? If yes, how?

14. What issues, if any, the use of *IFRCjobs* raises, in your compliance with policies, regulations, and laws, within your area of responsibility?

15. What are the implications of the social capability (e.g., Facebook, and LinkedIn) of IFRC*jobs* on records management?

16. How about the trustworthiness of records produced by IFRC*jobs*? How do you ascertain and guarantee the trustworthiness of these records, and what metadata has been generated to ensure their integrity?

17. What are your plans, if any, guiding the migration of records in/out of IFRC*jobs*? What difficulties, if any, did you encounter when migrating records into IFRC*jobs*? What are metadata requirements for records moved to the cloud? What are metadata requirements for records moved out of the cloud, including at the termination of service? Are organizational systems capable of ingesting records with their metadata from IFRC*jobs*?

18. How about long-term preservation of records produced by IFRC*jobs*? What requirements, if any, does your organization specify with respect to the long-term preservation of these records, such as, the format of the records?

19. The European Union is in the process of revising its data privacy law by replacing its Data Protection Directive 1995 with a new Data Protection Regulation, which is expected to be adopted this year. What do you think of the new Data Protection Regulation? How will the new Data Protection Regulation impact your organization's use of cloud-based service? How will the new Data Protection Regulation impact your organization's records/information policy?

20. What do you think are the responsibilities of records managers in the implementation and use of a cloud-based service like IFRC*jobs*?

II For Staff From Legal Department:

1. Were you involved in the evaluation and introduction of IFRC*jobs*? If so, in what way?

    a. What are the legal risks of using a cloud-based service like IFRC*jobs* in an international organization like yours?

    b. What legislations of your jurisdiction (e.g., privacy, disclosure, FOI, data security) did you consult when considering the adoption of a cloud-based service like IFRC*jobs*? Will entrusting data to the cloud put your organization in breach of these laws?

    c. Do you know where, juridically, your records are residing? Do you know what laws apply to data, information and records in the jurisdiction(s) in which your records are residing (e.g., evidence laws, FOI, national security)?

    d. What is your understanding of the risks to extraterritoriality and inviolability of records and archives when IFRC delegates its records to the cloud?

    e. Who owns the records created using IFRC*jobs*?

        i. Who owns the meta-data created by IFRC*jobs*?

    f. Who owns the copyright of the records produced by IFRC*jobs*?

        i. Who owns the copyright of the meta-data created by IFRC*jobs*?

    g. How is the privacy of data subjects protected as required by the laws IFRC needs to comply with?

    h. What measures did you adopt to mitigate the identified legal risks? (The measures can be discussed from these three perspectives, from service provider (e.g., service level agreement, quality of service), from end-user of the system (e.g., terms of agreement), and within your organization (e.g., organizational policy))

    i. Do you inform your applicants that IFRC*jobs* is a cloud-based service? Do you inform them that third parties may have access to their data? What other information do you give them concerning the risks accompanied in using IFRC*jobs*?

    j. So far, are these measures effective?

2. What are your major areas of concern when negotiating contract with the service provider? e.g., data access and portability, ownership of data. What are the major disagreements between you and the service provider? What do you think are the causes of these disagreements? How did you resolve them? Is your organization satisfied with the final contract? If no, why not? What resources did you consult when negotiating the contract? How do you monitor the compliance with the contract? What recommendations do you have to improve the negotiation between cloud service provider and user?
3. Since the introduction of IRFC*jobs*, have you encountered any new issues? If yes, what are they and how did you address them?
4. The European Union is in the process of revising its data privacy law by replacing its Data Protection Directive 1995 with a new Data Protection Regulation, which is expected to be adopted this year. What do you think of the new Data Protection Regulation? How will the new Data Protection Regulation impact your organization's use of cloud-based service?
5. What do you think are the responsibilities of legal department in the implementation and use of a cloud-based service like IFRC*jobs*?

III For Staff From Information Systems Department:

1. Which department within your organization initiated the adoption of IFRC*jobs*? What were your motivations for choosing a cloud-based service?
2. What system did you use previously for recruiting? What do you think are the differences between IFRC*jobs* and that system?
3. What are the benefits of using a cloud-based recruiting tool in relation to traditional in-house systems, and Application Service Provider (ASP) oriented applications?
    a. Are these benefits realized, e.g., cost reduction, scalability, elasticity, on-demand?
4. What are the risks of using a cloud-based recruiting tool in relation to traditional in-house systems, and Application Service Provider (ASP) oriented application?
5. What criteria did you use for selecting service provider? Did you consult any guidelines or checklists? If yes, what are they, and are they helpful? If no, why not, and would you like to have such tool?
6. How about the performance of IFRC*jobs*, e.g., availability, response time, security? Did you encounter any issues?
7. Technologically, what measures do you use to mitigate risks of cloud-based service? So far, are these measures effective?
8. What are your plans, if any, guiding the migration of records in/out of IFRC*jobs*? What difficulties, if any, did you encounter when migrating records into IFRC*jobs*? What are metadata requirements for records moved to the cloud? What are metadata requirements for records moved out of the cloud, including at the termination of service? Are organizational systems capable of ingesting records with their metadata from IFRC*jobs*?
9. How do you evaluate the service quality of IFRC*jobs*? Do you use any evaluation tool? If yes, what are they, and are they helpful? If they are not helpful, what recommendations do you have to improve such tools?
10. What about the security measures adopted by service provider for the physical servers, and records created? Are they at the same level with the security measured you used for your in-house servers and records?
11. Since the introduction of IRFC*jobs*, have you encountered any new issues? If yes, what are they, and how did you address them?
12. Are you considering using cloud-based service for other business functions? If yes, what are they?

13. What do you think are the impact of cloud-based service on your role as information technology specialists?
14. What do you think are the responsibilities of information technology department in the implementation and use of a cloud-based service like IFRC*jobs*?

IV For Staff From Risk & Audit Department:

1. Were you involved in the evaluation and introduction of IFRC*jobs*? If yes, in what way?
2. Did you do risk assessment when introducing IRFC*jobs*? If yes,
    a. Did you use any tool when doing risk assessment? If yes, what are they? If no, why not and would you like to have such tool?
    b. What are the sources of risk you identified? What are the areas of impacts? What are their potential consequences?
    c. What are the results of your risk analysis?
    d. Did the risk evaluation lead to a decision to treat the risk? Could you tell us more about your risk treatment plans?
3. Does IFRC*jobs* allow you or a third-party to do any auditing of their management of your data?
    a. If you are allowed to do such auditing, what tool do you use for such auditing? What are the areas that you audit?
    b. If a third-party will be allowed to do auditing, will the results be shared with you?
    c. If neither you nor a third-party will be allowed do auditing, how do you make sure that the service provider manages your data appropriately?
    d. How do you monitor the service quality of IFRC*jobs*?
    e. How does the service provider assure you of their compliance with the contract?
4. What are your opinions of the audit of cloud service?
5. What do you think are the responsibilities of the risk and audit department in the implementation and use of cloud-based service like IFRC*jobs*?

V For Staff From Human Resources Department

1. Were you involved in the evaluation and introduction of IFRC*jobs*? If yes, in what way?
2. How will you compare IFRC*jobs* with the previous system used for e-recruitment (i.e., JobNet) in terms of supporting recruitment work?
    a. *[Or if the interviewee has no experience with the previous system]* How will you evaluate IFRC*jobs* in terms of its capability in supporting recruitment work?

    b. How will you evaluate IFRC*jobs* in terms of capability in handling recruitment records, e.g., retrieval, use, publish, and disposal?

    c. How will you evaluate IFRC*jobs* in terms of its capability in protecting personal data of applicants?

    d. How about the social network capability of IFRC*jobs*?

    e. As far as you know, what are your applicants' perceptions of IFRC*jobs*? Do you inform them that IFRC*jobs* is a cloud-based recruitment tool? Have they expressed any concerns about the management of their personal data?
3. What do you think are the benefits of using a cloud-based recruitment tool like IFRC*jobs*?
    a. Are these benefits realized?
4. What do you think are the risks of using a cloud-based recruitment tool like IFRC*jobs*?
5. Does your organization make use of IFRC*jobs* through multiple devices such as mobile phones, and tablets? If yes, are these devices IFRC issued or employees'? Is there any policy in place on the use of multiple devices? What are the main concerns in the use of multiple devices?
6. What challenges, if any, did you encounter in the implementation of IFRC*jobs*?

Appendix B: NA 14 Draft Checklist for Cloud Contracts

InterPARES Trust Project

Research Report

Title:	Draft Checklist for Cloud Contracts
Status:	**DRAFT - Restricted (Internal IP Trust Researchers)**
Version:	1.1
Date submitted:	May 2015
Last reviewed:	May 2015
Author:	InterPARES Trust Project
Writer(s):	Jessica Bushey, Marie Demoulin, Elissa How and Robert McLelland
Research domain:	North American Team – Legal – NA14

The following Draft Checklist for Cloud Contracts v.1.1 is for internal use by InterPARES Trust Researchers. The target audience for this document is records managers and archivists assessing cloud services for their organization and/or institution. It is our hopes that IP Trust Researchers will utilize the Draft Checklist for Cloud Contracts v.1.1 in their projects and to provide feedback to Project 14 Team for the purposes of revision in the final report (due Fall/Winter 2015). The final Checklist will appear as an appendix in the Project 14 Final Report.

Draft Checklist for Cloud Contracts

Intended Audience: Records Managers and Archivists

Question	Y	N	?[3]	Notes
1. Agreement				
▪ Is the effective start date of the agreement clearly stated?				
▪ Is there an explanation of circumstances in which the services could be suspended?				
▪ Is there an explanation of circumstances in which the services could be terminated? (See also Section 8)				
▪ Is there an explanation of automatic notification, or an option to subscribe to a notification service, in the event of changes made to the terms governing the service?				
2. Data Ownership and Use				
▪ Do you retain ownership of the data that you store, transmit, and/or create with the cloud service?				
▪ Does the Provider reserve the right to use your data for the purposes of operating and improving the services?				
▪ Does the Provider reserve the right to use your data for the purposes of advertising?				
▪ Does the Provider's compliance with copyright laws restrict the type of content you can store with the cloud service?[4]				

[3] The "?" column indicates a situation in which the contract is unclear, or the question is not applicable to your situation.

[4] For example, the Digital Millennium Copyright Act (USA).

▪ Do you gain ownership of metadata generated by the system during procedures of upload, management, download, and migration?				
▪ Do you have the right to access these metadata during the contractual relationship? (See also Section 8)				
3. Availability, Retrieval, and Use				
▪ Are precise indicators provided regarding the availability of the service?				
▪ Does the degree of availability of the data meet your business needs?				
▪ Does the degree of availability of the data allow you to comply with freedom of information (FOI) laws?[5]				
▪ Does the degree of availability of the data allow you to comply with the right of persons to access their own personal data?[6]				
▪ Does the degree of availability of the data allow you to comply with the right of authorities to legally access your data for investigation, control, or judicial purposes?				
▪ Are the procedures, time, and cost for restoring your data following a service outage clearly stated?				
4. Data Storage and Preservation				
4.1. Data Storage				
▪ Does the Provider create backups of customer data?				
▪ In the event of accidental data deletion, does the Provider bear responsibility for data recovery?				
4.2. Data Preservation				
▪ Are there procedures outlined to indicate that your data will be managed over time in a manner that preserves their usability, reliability, authenticity, and integrity?				

[5] In general, freedom of information laws allow access by the general public to information held by national governments.

[6] In some countries there is a Privacy Act to protect the privacy of individuals with respect to personal information about themselves held by public *and/or* private bodies, and provide individuals with a right of access to that information.

▪ Are there procedures to ensure file integrity during transfer of your data into and out of the system (e.g., checksums)?				
▪ Is there an explanation provided about how the service will evolve over time (i.e., migration and/or emulation activities)?				
▪ Does the system provide access to audit trails concerning activities related to evolution of the service?				
▪ Will you be notified by the Provider of changes made to your data due to evolution of the service?				
▪ Can you request notification of impending changes to the system related to evolution of the service that could impact your data?				
5. Data Retention and Disposition				
▪ Will your data (and all their copies) be destroyed in compliance with your data retention and disposition schedules?				
▪ If so, will they be immediately and permanently destroyed in a manner that prevents their reconstruction, according to a secure destruction policy ensuring confidentiality of the data until their complete deletion?				
▪ Are you aware of the nature and content of the associated metadata generated by the system?				
▪ Will the Provider destroy associated metadata upon disposition of your data?				
▪ Will the Provider deliver and/or give access to audit trails of the destruction activity?				
▪ Will the Provider supply an attestation, report, or statement of deletion (if required by your internal or legal destruction policies)?				
6. Security, Confidentiality, and Privacy				
6.1. Security				
▪ Does the system prevent unauthorized access, use, alteration, or destruction of your data through technical, physical, and organization measures?				
▪ Is your data secure during procedures of transfer into and out of the system?				
▪ Does the system provide and give you access to audit trails, metadata, and/or access logs to demonstrate security measures?				

▪ Will you be notified in the case of a security breach or system malfunction?				
▪ Does the Provider use the services of a subcontractor?				
▪ Does the Provider offer information about the identity of the subcontractor and its tasks?				
▪ Is there a disaster recovery plan available?				
6.2. Confidentiality				
▪ Does the Provider have a confidentiality policy in regards to its employees, partners, and subcontractors?				
6.3. Privacy				
▪ Are there privacy, confidentiality, or security policies for sensitive, confidential, personal or other special kinds of data you store with the Provider?				
▪ Does the system prevent unauthorized access, use, alteration, or destruction of your personal information through technical, physical, and organizational measures?				
▪ Is it clearly stated what personal information is collected and why it is collected?				
▪ Is it clearly stated how the personal information collected will be used?				
▪ Does the Provider share your personal information with other companies, organizations, or individuals without your consent?				
▪ Does the Provider clearly state the legal reasons it which they would share your personal information with other companies, organizations, or individuals?				
▪ If the Provider shares your personal information with their affiliates for processing reasons, is this done in compliance with a privacy, confidentiality, or security policy?				
6.4. Accreditation and Auditing				
▪ Is the Provider accredited with a third party certification program?				
▪ Is the Provider audited on a systematic, regular, and independent basis by a third-party in order to demonstrate compliance with security, confidentiality, and privacy policies?				
▪ Is such a certification or audit process documented?				

▪ Do you have access to information such as the certifying or audit body and the expiration date of the certification?				
7. Data Location and Cross-border Data Flows				
7.1. Data Location				
▪ Do you know where your data and their copies are located while stored in the cloud service?				
▪ Does it comply with the location requirements that might be imposed on your organization's data by law, especially by applicable privacy law?				
▪ Do you have the option to specify the location, in which your data and their copies will be stored?				
7.2. Cross-border Data Flows				
▪ Will you be notified if the data location is moved outside your jurisdiction?				
▪ Is the issue of your stored data being subject to disclosure orders by national or foreign security authorities addressed?				
▪ Does the Provider clearly state the legal jurisdiction in which the agreement will be enforced and potential disputes will be resolved?				
8. End of Service – Contract Termination				
▪ In the event that the Provider terminates the service, will you be notified?				
▪ Is there an established procedure for contacting the Provider if you wish to terminate the contract?				
▪ If the contract is terminated, will your data be will be transferred to you in a usable and interoperable format?				
▪ Is the procedure, cost, and time period for returning your data at the end of the contract clearly stated?				
▪ At the end of the contract, do you have the right to access the associated metadata generated by the system?				
▪ At the end of the contract and after complete acknowledgement of restitution of your data, will your data and associated metadata be immediately and permanently destroyed, in a manner that prevents their reconstruction?				

Appendix C: NA 06 Retention & Disposition Functional Requirements

InterPARES Trust
North American Team
Research Project 06
Retention & Disposition in a Cloud Environment
http://interparestrust.org

March 2015

When using this questionnaire, please cite as
InterPARES Trust (2015) Retention & Disposition Functional Requirements. North American Team Research Project 06. March 2015.

Retention & Disposition Functional Requirements

Questionnaire for use when evaluating specific cloud products/services

No.	Questions	Yes	No	Don't Know
Privacy and Security Considerations				
1	Does the vendor allow independent audits of systems and processes?			
2	Is the content encrypted when in transit to the cloud?			
3	Is the content encrypted when at rest in the cloud?			
4	Are the physical servers located within a jurisdiction approved for your organization?			
5	Are the backup servers located within a jurisdiction approved for your organization?			
Establishing disposition authorities				
6	What indexing capability is supported (can it accommodate customers' taxonomy for indexing)?			
7	Can retention periods be applied?			
8	Can destruction be automated?			
Applying disposition authorities				
9	Can a disposition authority (retention and disposition specifications) be applied to aggregations of records?			
10	Can records be locked down for viewing only?			
11	Can records be retained indefinitely?			
12	Can records not in an aggregation be destroyed at a future date?			
13	Can records not in an aggregation be transferred at a future date?			
Executing disposition authorities				
14	Can records be deleted according to the retention/disposition schedule?			
15	Can backups be deleted according to the retention/disposition schedule?			
16	Are users alerted to conflicts related to links from records to be deleted to other records aggregations that have different records disposition			

	requirements?			
17	If more than one disposal authority is associated with an aggregation of records, can these multiple retention requirements be tracked to allow the manual or automatic lock or freeze on the process (ex. Freeze for litigation or freedom of information request)?			
Documenting disposal actions				
18	Are disposal actions documented in process metadata?			
19	Can all disposal actions be automatically recorded and reported to the administrator?			
Reviewing disposition				
20	Are electronic aggregations presented for review along with their records management metadata and disposal authority information so both content and records management metadata can be reviewed?			
21	Can records be marked for destruction, transfer, further review?			
22	Are all decisions made during review stored in metadata?			
23	Can the system generate reports on the disposition process?			
24	Is the ability to interface with workflow facility to support scheduling, review, and export transfer processes provided or supported?			
Integration				
25	Is the metadata schema compatible with other systems, such as Enterprise Content Management or Records Management Systems?			