JIU/REP/2019/5

United Nations

Managing cloud computing services in the United Nations system

Report of the Joint Inspection Unit

Prepared by Jorge T. Flores Callejas and Petru Dumitriu

JIU/REP/2019/5
Original: English

Managing cloud computing services in the United Nations system

Report of the Joint Inspection Unit

Prepared by Jorge T. Flores Callejas and Petru Dumitriu

United Nations • Geneva, 2019

Executive summary

Managing cloud computing services in the United Nations system (JIU/REP/2019/5)

The Joint Inspection Unit (JIU) conducted this review as part of its programme of work for 2018. The review originated from a proposal made by the Inspectors and its scope was system-wide, as it covered all of the JIU United Nations participating organizations. The Inspectors also examined the relationship between the organizations of the United Nations system and the United Nations International Computing Centre (UNICC), given its particular role providing information technology services, support and solutions to several organizations of the United Nations system.

Background

The need to use new technologies is one of the most frequently expressed throughout the 2030 Agenda for Sustainable Development. Expectations are high, as also heralded in the Secretary-General's strategy on new technologies or in the International Labour Organization's report entitled *Work for a Brighter Future: Global Commission on the Future of Work*. It is imperative that the organizations of the United Nations system deepen their own understanding of the challenges raised by technologies at the global level and, equally importantly, expand and diversify their internal knowledge and exposure to them.

Cloud computing is one such technology. In recent years, cloud computing has become a major trend not only in the private sector, but also in the operational reality of United Nations organizations. The introduction of more technology into all spheres has always raised discussions. Cloud computing, like other technologies, is associated with high expectations and opportunities, which have been promoted very energetically by the service suppliers.

The terms "cloud" and "cloud computing" refer broadly to the concepts of remote or distributed computing via broadband networks and/or the Internet. In its general sense, the term "cloud computing" describes the provision of computing services through a network from a distant source.

The use of cloud computing systems has grown considerably in the past decade and almost all of the United Nations organizations are already using a variety of cloud computing services, such as email, hosting of public websites, recruitment and talent management applications, and collaboration tools. The use of cloud computing technology not only provides cost benefits, but also makes data accessible on different devices, including mobile devices, from any location and at any time. Cloud computing has many other potential benefits, as discussed in the present review; however, it also comes with risks.

The risks involved are qualitatively new and directly related to the distributed and shared nature of cloud computing. Such risks include issues related to data confidentiality and, in the case of the United Nations and the specialized agencies, to the need to safeguard the provisions of the Convention on the Privileges and Immunities of the United Nations (1946) and the Convention on the Privileges and Immunities of the Specialized Agencies (1947) respectively. Consequently, the risks need to be carefully assessed and balanced against the potential benefits when the introduction of cloud solutions is being contemplated.

In the present report, the Inspectors intend, inter alia, to argue for a more balanced approach in facing the potential benefits of the cloud, considering associated specific risks, and the potential synergies from a United Nations system-wide perspective that could be achieved by maximizing the potential of UNICC, a specialized entity created precisely to serve the system.

The Inspectors also proposes a number of additional safeguards and advice in an effort to expand the United Nations common knowledge on cloud computing, to increase the level of inter-agency cooperation and to strengthen the negotiating capacity of the United Nations organizations.

The main users of the review are all participating organizations and Member States. The review was undertaken in an effort to inform their policy-setting role while facilitating their monitoring and assessment of relevant activities. The sharing of best practices and information across the United Nations system will contribute to strengthening coordination and understanding of the different cloud computing initiatives undertaken.

Use of cloud computing by United Nations organizations

The United Nations system presently exhibits a full range of cloud adoption models and stages of development, and, consequently, different degrees of maturity. A small number of organizations do not use cloud computing at all, whereas others have information and communications technology (ICT) strategies that are strongly based on cloud services and resources, promoting a "cloud-first" approach. Between the two extremes, there are many organizations that use the cloud to a certain extent. Still, some general and technical trends can be identified as common to a number of organizations.

Cost reduction, simplification, flexibility, agility, better perceived security and innovation are among the most important reasons quoted by organizations for their shifting from traditional information systems to cloud-based services. Another reason for shifting to the cloud is the fact that certain business applications are often no longer available, or available as cloud services only.

Overall, the United Nations system follows the wider trend of commodification of computing services and cloud adoption. The primary driving forces and considerations for using cloud services are often similar to those of enterprises worldwide. Specific conditions related to the nature of United Nations organizations rarely have an impact on the decision to use cloud computing.

Need for contextual risk analysis

The United Nations organizations are well aware of the risks associated with cloud computing, as confirmed by answers provided to the JIU corporate questionnaire and the interviews held by the Inspectors. However, the Inspectors would like to stress that when contemplating cloud-based solutions, United Nations organizations should carry out their own risk analysis, taking into consideration their specific context. Besides differing needs, organizations also show differing levels of risk tolerance. An acceptable risk to one organization is often not acceptable to another. As the business and regulatory frameworks change and new risks arise, risk assessments should be a regular activity and a key mandatory step in any consideration of cloud computing solutions.

There are some inherent security risks specific to the cloud environment, which can be assessed, managed and deemed acceptable for several use cases and organizations. There are also security advantages in the cloud for certain use cases, such as for agencies operating in geographically dangerous locations. Like on-premises data centres, cloud environments can be made more secure or less secure by clients' and vendors' choices. The public cloud offerings of the biggest providers, which currently host the majority of United Nations system's data, are not the only option, and the organizations could be looking at complementary options to reduce strategic risks for the United Nations community as a whole.

Cloud computing as a tool to achieve higher integration and compatibility among United Nations organizations

As cloud deployment increases and matures in the United Nations system, the importance of compatibility among the different cloud services deployed, including their interoperability and portability, is likely to grow. This is of particular relevance in the context of increased inter-agency collaboration and the current Secretary-General's reform efforts, including interoperability in the field. In the view of the Inspectors, there is a need for further collaboration and coordination among United Nations organizations operating in the field, with the final objective of developing the required compatibility and interoperability of ICT platforms and systems that will ultimately facilitate joint and/or closely coordinated planning and operations. While this issue is not purely technical and depends on complex

coordination, a suitable technology could play an enabling role. Cloud computing may be one important tool to achieve this end.

A new financing model for computing services

The transition from conventional to cloud-based computing requires a change in the structural financing of ICT services. By leveraging shared infrastructure and economies of scale, cloud computing offers a compelling business model. Traditional ICT services require significant up-front capital investments in computing hardware, software, communications infrastructure and the data centre environment in which it is hosted. These are followed by recurrent and relatively evenly distributed operating costs, maintenance, support, upgrades, migration, disaster recovery, backup and so on. With cloud computing, the initial capital investment is replaced by a pay-per-use model; there is no initial capital investment required and fixed costs are transformed into operating costs. While this is often seen as an advantage of the cloud computing model, it also holds certain disadvantages and unfulfilled promises.

Data privacy challenges and the need to protect the privileges and immunities of the United Nations organizations.

Cloud computing enables global availability of information; however, its intrinsic nature, characterized by remote access and distributed processing, poses risks concerning data and information privacy. Protecting data and information is imperative to Governments, organizations and enterprises worldwide. In the view of Inspectors, digitalized data are a form of assets, which are referred to in the provisions of the Convention on the Privileges and Immunities of the United Nations and the Convention on the Privileges and Immunities of the Specialized Agencies. Thus, any information owned by United Nations entities and stored by third parties, regardless of the storage location, should be subject to these immunities, which, given their international and high-level nature, may override the prevailing applicable national and regional regulations.

Enhancing accountability through service level agreements

The use of cloud computing is more than a technological challenge. It may also have a significant impact on organizational change management, affecting different aspects of the governance, security, efficiency and financing of organizations. Consequently, there is an evident need for comprehensive decision-making practices that include the different organizational units and go beyond technical considerations when contemplating cloud-based services. Furthermore, given the challenges posed by cloud services and the appearance of third-party actors, the selection and use of cloud-based services requires the establishment of appropriate due diligence processes and the preparation of comprehensive contracts, or service-level agreements (SLAs), which must be seen not only as a legal protection mechanism but also as a tool to effectively manage relations with cloud vendors on the basis of objective output metrics. The Inspectors firmly believe that United Nations organizations should actively monitor SLAs and hold vendors accountable for failure to comply with the requirements established.

United Nations International Computing Centre: an opportunity to strengthen coordination on information and communications technology and enhance effectiveness across the United Nations system

The Inspectors encourage United Nations organizations and UNICC to find areas of cooperation in which shared services could be provided at a reasonable cost using the UNICC hub to leverage its expertise and complement that of the organizations without requiring additional and costly expertise in-house within each organization. While United Nations organizations should consider using UNICC, the Inspectors recognize the individuality of each organization: it is the ultimate responsibility of the organizations to make relevant decisions based on their operational and specific needs.

Data and information security is one major challenge faced by all organizations using cloud computing. The Inspectors believe that it would make sense to have a comprehensive United Nations system-wide approach to information security. In their view, this cannot be accomplished without the contribution and coordinated use of UNICC, which already offers security services and is actively working on further expanding its cybersecurity services.

Many factors discussed in the present review point to opportunities for furthering cooperation in the context of more strategic and coordinated use of ICT resources by United Nations organizations. The Inspectors believe that UNICC could and should be one of the pillars supporting the digital transition, including the use of cloud computing. In fact, the characteristics inherent to cloud computing are conducive to the implementation of the UNICC mandate as the ICT shared services provider of the United Nations system.

UNICC holds unrealized potential as the strategic United Nations hub for supplying third-party public cloud services to partner organizations. Joint access to public cloud services could provide further cost savings, from a system-wide perspective, and leverage negotiation capacity.

UNICC could offer additional opportunities in its potential role as a cybersecurity hub for partner organizations to make their use of cloud services safer and their emergency response more effective. While security services are already offered by UNICC, there is still potential for bigger gains in this area, for the system as a whole, if more organizations join the hub. A number of security services become more effective when there are more participants sharing information and collaborating on data and application security.

Recommendation addressed to the General Assembly

The Inspectors are of the opinion that in order for UNICC to achieve its full potential and be able to focus in a strategic way on the digital transformation of the United Nations system as a whole, the UNICC Management Committee should be strengthened through the incorporation of senior management into its membership.

In this regard, the following recommendation is addressed to the General Assembly for endorsement:

Recommendation 5. The General Assembly of the United Nations should review and update the mandate of UNICC, and consider, inter alia, diversifying the membership of the UNICC Management Committee and delegating appropriate levels of authority with respect to decision-making on digital information technologies, including cloud computing initiatives.

Recommendation addressed to legislative and governing bodies of United Nations organizations

Recommendation 2. The governing bodies of the United Nations organizations should request the heads of their respective organizations to include provisions in their financial strategies that facilitate the adaptation, responsiveness and efficient use of operational expenditures and capital investments related to new technologies.

Recommendations addressed to executive heads of United Nations organizations

Recommendation 1. The executive heads of the United Nations organizations should ensure that business continuity planning includes strategies and measures to mitigate the risk of failure by cloud service providers to deliver the contracted services.

Recommendation 3. The executive heads of the United Nations organizations should put in place periodic procedures to ensure that their corporate ICT strategies, including those for cloud computing services, are aligned with the organizations' business needs and priorities, and yield value for the investment.

Recommendation 4. The executive heads of the United Nations organizations should ensure that a comprehensive risk analysis exercise is undertaken before contracting ICT services, including cloud-based services. The risk analysis exercise should consider both technical and financial risks and benefits, and relevant safeguards should be included in the service-level agreement.

Contents

Abbreviations

AWS	Amazon Web Services
CEB	United Nations System Chief Executives Board for Coordination
ERP	enterprise resource planning
FAO	Food and Agriculture Organization of the United Nations
IaaS	Infrastructure as a Service
IAEA	International Atomic Energy Agency
ICAO	International Civil Aviation Organization
ICT	information and communications technology
IEC	International Electrotechnical Commission
ILO	International Labour Organization
IMO	International Maritime Organization
ISO	International Organization for Standardization
ITC	International Trade Centre
ITU	International Telecommunication Union
JIU	Joint Inspection Unit
NIST	National Institute of Standards and Technology (United States of America)
PaaS	Platform as a Service
PAHO	Pan American Health Organization
PASB	Pan American Sanitary Bureau Management Information System
SaaS	Software as a Service
SLA	service-level agreement
UNAIDS	The Joint United Nations Programme on HIV/AIDS
UNCTAD	United Nations Conference on Trade and Development
UNDP	United Nations Development Programme
UNEP	United Nations Environment Programme
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNFPA	United Nations Population Fund
UN-Habitat	United Nations Human Settlements Programme
UNHCR	Office of the United Nations High Commissioner for Refugees
UNICC	United Nations International Computing Centre
UNICEF	United Nations Children’s Fund
UNIDO	United Nations Industrial Development Organization
UNODC	United Nations Office on Drugs and Crime
UNON	United Nations Office at Nairobi
UNOPS	United Nations Office for Project Services
UNOV	United Nations Office at Vienna
UNRWA	United Nations Relief and Works Agency for Palestine Refugees in the Near East
UN-Women	United Nations Entity for Gender Equality and the Empowerment of Women
UNWTO	World Tourism Organization

UPU	Universal Postal Union
WFP	World Food Programme
WHO	World Health Organization
WIPO	World Intellectual Property Organization
WMO	World Meteorological Organization

I. Introduction

A. Background

1. The Joint Inspection Unit (JIU) of the United Nations system conducted the present review as part of its programme of work for 2018. The review originates from an internal proposal made by the Inspectors; however, its topic is related to those of other proposals received from participating organizations, such as information and communications technology (ICT) governance, cybersecurity and big data management.

2. The use of appropriate state-of-the-art technologies is key for the efficient management and operation of modern organizations. In its resolution 68/198 of 20 December 2013, the General Assembly refers to cloud computing for the first time, "[n]oting that progress and many innovations in the field of information and communications technologies, such as mobile Internet, social networking and cloud computing, contribute to a dynamic landscape that requires that all stakeholders continuously adapt to such innovations". Key technologies underpinning the evolving digital economy include advanced robotics, artificial intelligence, the Internet of things, cloud computing, big data analytics and three-dimensional printing.[1] The shift towards cloud computing can be seen as a step change in the relationship between telecommunications, businesses and society as a result of massively enhanced processing power, data storage and higher transmission speeds, accompanied by price reductions.[2]

3. Cloud computing involves the use of computing and ICT resources that are delivered as a service over the Internet from geographically disparate locations, using a shared and dynamically scalable infrastructure.[3]

4. The use of cloud computing systems has grown considerably in the past decade and almost all of the United Nations organizations are already using a variety of cloud computing services, such as email, hosting of public websites, recruitment and talent management applications, and collaboration tools. The use of cloud computing technology not only provides cost benefits, but also makes data accessible on different devices, including mobile devices, from any location and at any time. Cloud computing has many other benefits, as discussed in subsequent chapters; however, like all new technologies, it also comes with risks. The main risks associated with cloud computing are those inherent to traditional information systems using remote and distributed processing, with data and information travelling over broadband networks and/or the Internet, as well as those risks taken with outsourced service provisioning where one or several third-party actors (cloud service providers) intervene.

5. Furthermore, some of the risks are qualitatively new and directly related to the distributed and shared nature of cloud computing. Such risks include issues related to data confidentiality and, in the case of the United Nations and the specialized agencies, to the need to safeguard the provisions of the Convention on the Privileges and Immunities of the United Nations (1946)[4] and the Convention on the Privileges and Immunities of the Specialized Agencies (1947)[5] respectively. Cloud computing poses an information security risk, and a growing reliance on cloud computing is prompting concerns over security, privacy and ownership of user data. It can also give the companies that control the data considerable market power, causing concerns about potential market dominance.[6] Since the cloud

[1] *Information Economy Report 2017: Digitalization, Trade and Development*, (United Nations publication, Sales No. E.17.II.D.8).

[2] Ibid.

[3] Information Security Special Interest Group, Chief Executives Board for Coordination, "Use of cloud computing in the United Nations system: recommendations for risk mitigation", white paper, June 2013, p. 4.

[4] General Assembly resolution 22 A (I).

[5] General Assembly resolution 179 (II).

[6] *Information Economy Report 2017*.

computing market is dominated by a small number of major players, there is a high risk of monopolistic behaviour. High vendor dependence and consequently low negotiation power are challenges confirmed by some professional associations. Consequently, the risks need to be carefully assessed and balanced against the potential benefits when the introduction of cloud solutions is being contemplated. Zero risk does not exist. This review is intended, inter alia, to add value and provide support to organizations in their consideration of cloud computing initiatives.

B. Objectives and scope

6. The main objectives of this review are:

(a) To analyse the different cloud computing frameworks, strategies, policies and practices in selected United Nations organizations, with a view to identifying valuable information regarding best practices, innovative approaches and lessons learned and thereby promoting effective cloud computing governance. The key aspects to consider are the current ICT and cloud computing governance structures in place, and the strategic alignment of cloud computing with the existing ICT strategies and with the organizations' business objectives and mandates;

(b) To examine and identify specific security and data privacy issues arising from the use of cloud computing, as well as current risk management mechanisms, including business continuity and disaster recovery plans;

(c) To examine cloud computing governance at the United Nations system-wide level, notably coordination and cooperation within the system, such as through the Digital and Technology Network and other relevant mechanisms.

(d) To disseminate best practices, including ideas and recommendations to inform the development of safeguards in using cloud computing services.

7. The review is system-wide by definition; it covers all JIU-participating organizations and their relationship with the United Nations International Computing Centre (UNICC), given its particular role in providing information technology services, support and solutions to several organizations of the United Nations system. The review also refers to other international organizations that have developed cloud computing frameworks, strategies and practices, in an effort to illustrate good practices and lessons learned.

8. The review does not address cloud computing from a technical perspective and does not cover a specific period of time. Its focus is on recent cloud computing developments within the United Nations system, current issues faced by organizations and forward-looking initiatives.

9. The main users of the review are all participating organizations and Member States; it is intended to provide value to all participating organizations, regardless of their size. The sharing of best practices and information across the United Nations system will contribute to strengthening coordination and understanding of the different cloud computing initiatives undertaken. The review is also addressed to Member States in an effort to inform them in their policy-setting role while facilitating their monitoring and assessment of relevant activities.

C. Methodology

10. The methodology used combines qualitative and quantitative approaches to data collection and analysis. The review began with the preparation of preliminary terms of reference, which were further updated using the output of meetings with representatives of participating organizations and Member States. A desk review of documentation available was undertaken, followed by a data-collection phase that included the preparation of corporate questionnaires and interviews with relevant actors. The Inspectors conducted missions to New York, Rome, Vienna and Washington, D.C., and met with relevant officials of the Geneva-based organizations. Once finalized, the data-collection phase was followed

by in-depth analysis of data gathered. Given the technical nature of the review, a specialized consultant was hired to provide technical support to the JIU team. For quality assurance purposes, an internal peer review ("collective wisdom") method was used to solicit comments from the JIU Inspectors on the draft report, which was subsequently circulated to the organizations concerned for substantive comments on the findings, conclusions and recommendations, as well as for the correction of any factual errors.

D. Cloud computing: concepts and definitions

11. As previously indicated, the review does not cover cloud computing from a technical perspective. However, the technical nature of the subject requires the use and understanding of some basic concepts specific to cloud computing. The cloud concepts, definitions and terminology used in this review follow those established by the National Institute of Standards and Technology (NIST) of the United States of America.[7]

12. The terms "cloud" and "cloud computing" refer broadly to the concepts of remote or distributed computing via broadband networks and/or the Internet. For example, the International Telecommunication Union (ITU) and the International Organization for Standardization (ISO) define cloud computing as "a paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on demand".[8] In an effort to facilitate a common understanding, NIST issued in 2011 its standard definition[9] (see box 1) and reference architecture on cloud computing[10]. Both are in the form of special publications, which are not official United States government standards but are designed to provide guidance to communities of practitioners and researchers.

Box 1

National Institute of Standards and Technology, definition of cloud computing

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

13. The cloud computing model is composed of five essential characteristics, three service models and four deployment models.[11] Any cloud system recognized as such should be characterized by all of these essential characteristics and be deployed and offered using at least one of the defined models. These elements and models are explained in the boxes 2 to 4 below using the NIST definitions and concepts (see also figure I). The Inspectors note that cloud computing should no longer be seen merely as an ICT issue, but also as a governance challenge and a business model issue with multiple implications.

[7] Under the umbrella of the United States Department of Commerce, NIST aims to promote innovation and industrial competitiveness by advancing measurement science, standards and technology. See www.nist.gov/about-nist/our-organization/mission-vision-values.

[8] International Electrotechnical Commission (IEC), ISO and ITU, "Information technology: cloud computing – overview and vocabulary", international standard ISO/IEC 17788:2014 (E)– recommendation ITU-T Y.3500 (08/2014), p. 4.

[9] Peter Mell and Timothy Grace, "The NIST definition of cloud computing: recommendations of the National Institute of Standards and Technology", Special Publication 800-145, September 2011.

[10] Fang Liu and others, "NIST cloud computing reference architecture: recommendations of the National Institute of Standards and Technology", Special Publication 500-292, September 2011.

[11] Nayan B. Ruparelia, *Cloud Computing* (Cambridge, Massachusetts, MIT Press, 2016).

Box 2

Essential characteristics of a cloud computing system: National Institute of Standards and Technology

On-demand self-service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

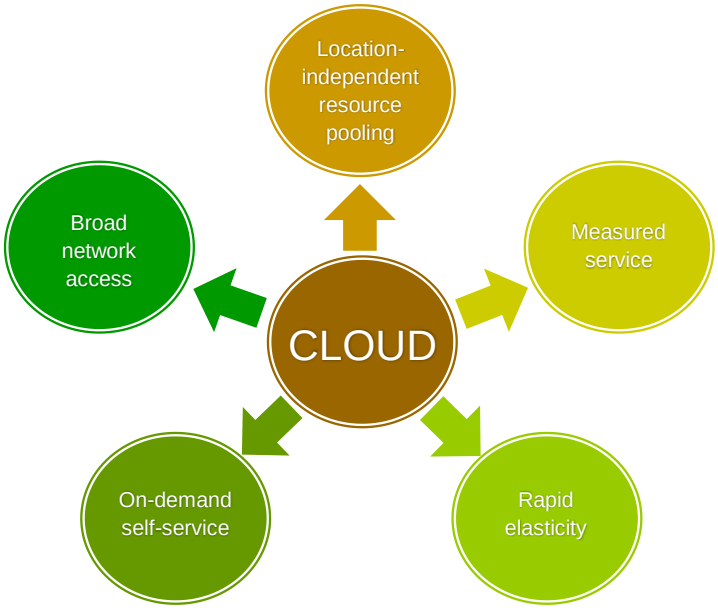
Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (such as mobile phones, tablets, laptops, and workstations).

Resource pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (for example, country, state or data centre). Examples of resources include storage, processing, memory and network bandwidth.

Rapid elasticity. Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outwards and inwards commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (for example, storage, processing, bandwidth and active user accounts). Resource usage can be monitored, controlled and reported, providing transparency for both the provider and the consumer of the utilized service.

Figure I
Cloud computing: essential features



Source: Ray Rafaels, Cloud Computing: From Beginning to End – Complete Guide on Cloud Computing Technology and Methodologies to Migrate to the Cloud (CreateSpace Independent Publishing Platform, 2015).

14. Cloud computing in its general sense describes the provision of computing services through a network from a distance source. One important aspect of this concept is the access control and the ownership of the computing infrastructure and resources that are being

provided as a service. The review distinguishes between different deployment and service models offered, given that the choice of a specific model has important implications in that the ownership of the infrastructure, security and associated risks are substantially different for different deployment models. There are four primary cloud computing deployment models: private cloud, community cloud, public cloud and hybrid cloud.

Box 3

Cloud computing deployment models: National Institute of Standards and Technology definitions

Private cloud. The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (such as business units). It may be owned, managed and operated by the organization, a third party or some combination of them, and it may exist on or off premises.

Community cloud. The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (such as mission, security, policy and compliance considerations). It may be owned, managed and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud. The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed and operated by a business, academic or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability.

15. The term "public cloud" typically refers to publicly available services offered by commercial providers. These providers build and maintain the necessary infrastructure and charge for the services used. To maximize the use of resources (and thus reduce costs), cloud providers dynamically facilitate the shared use of their computing resources. Public cloud is the most frequently used deployment model among organizations. In order to illustrate the impact of deployment models, it is important to note that private clouds are more secure than other alternatives given that the computing resources (that is, the hardware and software) are controlled and used by a single organization. However, with public clouds in particular, where the cloud infrastructure is owned by a third party, there is a risk that classified or sensitive data located outside a country's borders and data is processed and stored in infrastructure shared with other external users. There is also a higher risk of an external threat (cyberattack). The benefits and risks of cloud computing are discussed later in the review.

16. In addition to the deployment models, there are three basic service models, which define the boundaries and responsibilities of the cloud service provider and the client with respect to the use of the hardware infrastructure, associated middleware and software applications: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Like in the case of the deployment models, the selection of the service model has important implications for, inter alia, the security of cloud computing systems.

Box 4

Cloud computing service models:
National Institute of Standards and Technology definitions

Infrastructure as a Service (IaaS). The capability provide d to the consumer is to provision processing, storage, networks and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage and deployed applications; and possibly limited control of select networking components (such as host firewalls).

Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (for example, web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

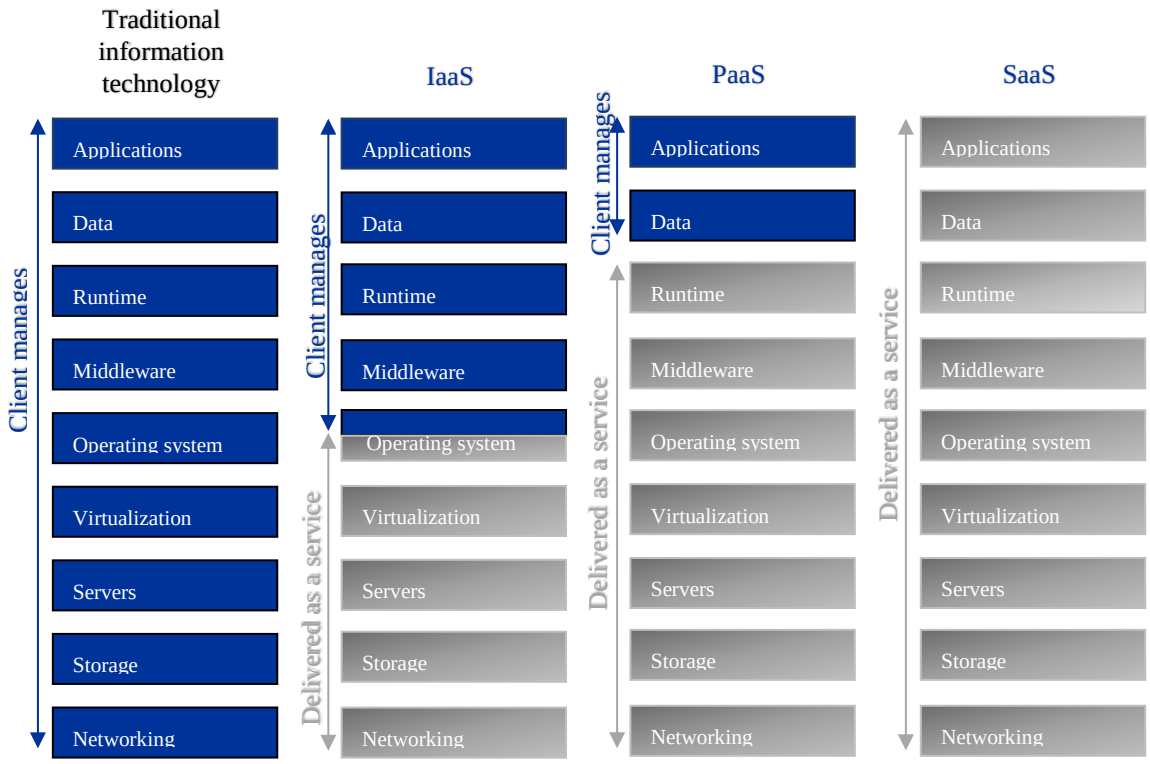
17. The three major service models address different client needs and focus on the provision of different computing segments. While there are some intended benefits of cloud computing that are common to all service models (such as cost reduction), each of them has its specific objectives and properties (see also figure II):

(a) IaaS replaces the client's computing and networking hardware with raw computing resources delivered online, from the cloud (distant data centres), via the Internet;

(b) PaaS replaces the hardware, as well as some layers of middleware and software, providing a client with a ready-made application development platform from the cloud where the client can develop, test and run its own applications;

(c) SaaS delivers complete functionality of applications from the cloud, where all the layers (hardware, networking and software) are managed by the provider. The client mainly uses the applications developed and serviced by the provider.

Figure II
Different cloud service models: IaaS, PaaS, SaaS



Source: https://blogs.msdn.microsoft.com/dachou/2018/09/28/cloud-service-models-iaas-paas-saas-diagram/

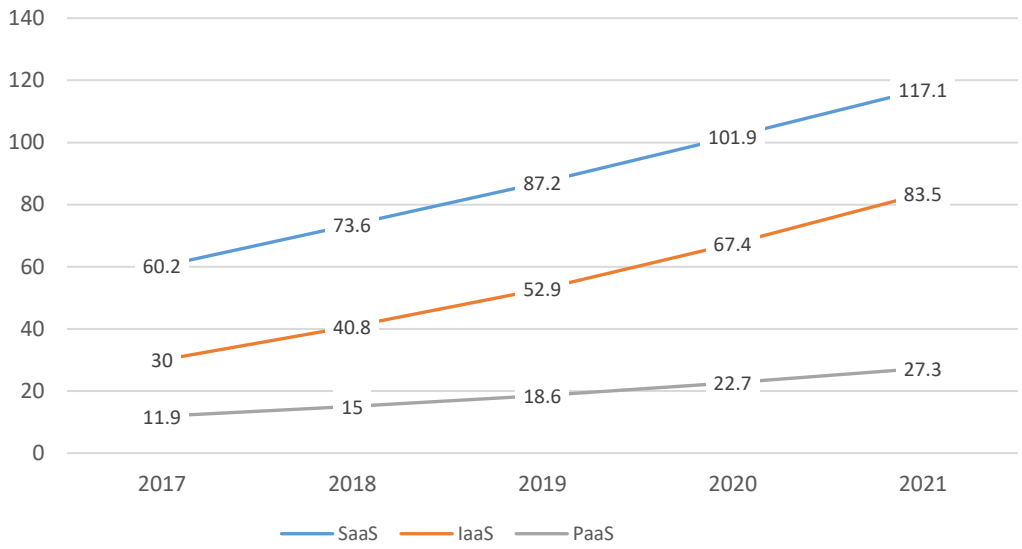
18. Cloud computing services continue to evolve, which makes it difficult to categorize some of them as belonging to only one of the above service categories. In practice, other variants of service models have emerged, such as “information as a service” and “business process as a service”. Often specialized, such services cross the borders of the conventional division into infrastructure, platform and software services provided from the cloud, frequently combining elements from different service models into one product. This trend will continue and further blur the borders between the principal service models.

E. Overview of the cloud market

19. In 2018, the public cloud market continued to grow and mature. Among the leading providers, year-to-year quarterly growth rates reached up to 80 per cent for some service segments. This trend shows that commodification of computing services by enterprises is becoming increasingly widespread worldwide.

20. In the sphere of generic cloud services, one of the most important current trends is the market dominance of a handful of major providers. Among such providers, Microsoft and Amazon have achieved the highest growth rates and the largest market shares. According to recent industry reports, the top five IaaS providers, led by Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform, account for about 80 per cent of all IaaS sales globally, depending on the different metrics used by analysts. Figure III provides an illustration of the current market size and projected market growth until 2021.

Figure III
Cloud market revenue and projected market growth
(Billions of United States dollars)



Source: https://www.skyhighnetworks.com/cloud-security-blog/microsoft-azure-closes-iaas-adoption-gap-with-amazon-aws/

21. Similarly, for the most common and widely used SaaS services, such as email, office productivity and document storage, a small number of large-scale providers – Microsoft and Google – dominate the market segment. The market offer is more diverse when it comes to specialized business applications running in the SaaS cloud. This includes various applications relating to customer relationship management, human resources, payroll and similar that are offered as cloud services.

22. However, it should be noted that in some cases, apparently independent SaaS providers and services rely on the infrastructure of the large IaaS providers mentioned above, which results effectively in an even higher concentration of cloud data in the private data centres of the few biggest IaaS providers.

Main suppliers of the United Nations organizations

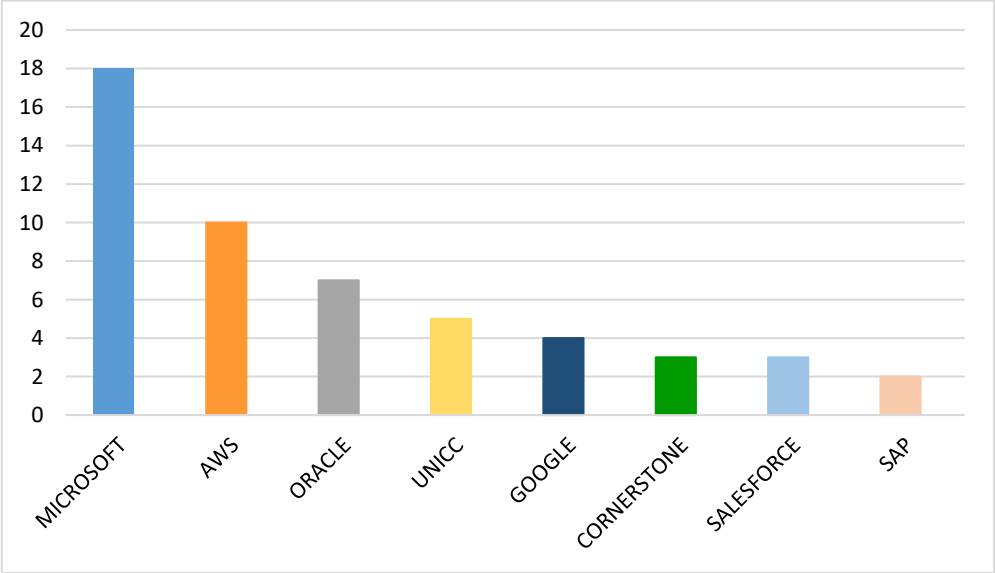
23. It is not surprising that the main cloud suppliers used by United Nations organizations are the same few companies that lead the cloud computing market worldwide. For general services, Microsoft and AWS are used most often. For business applications, the major providers are Oracle, Cornerstone, Systems Applications and Products in Data Processing (SAP) and Salesforce. Annex II contains an overview of the current use of specific cloud computing services used by the United Nations organizations.

24. Microsoft is the leading cloud provider for the United Nations organizations, used by 18 out of 25 respondents (72 per cent). The majority of organizations use it for its SaaS services: cloud-based email hosting and Office 365 productivity suite. SaaS applications are widely used across the system and Microsoft Office 365 is probably the most popular. AWS was the first large-scale provider to package and offer self-provisioning of virtual servers – a typical IaaS offer – in a relatively simple and commodified manner. It is currently used by 10 respondents (40 per cent). However, AWS does not offer a broad set of services under the SaaS model, for which demand is growing among respondent organizations, and in many cases determining organization's choice of supplier.

25. Figure IV shows the number of participating organizations using major cloud service providers. It is important to note a single organization may use one or more providers for different cloud services (email, hosting of public websites and so on) at the same time. Some of the cloud-oriented services provided by UNICC and the United Nations Secretariat mean that they qualify as community cloud providers for the United Nations system.

Figure IV
Cloud services providers for United Nations organizations

(Number of organizations)



26. United Nations entities use cloud computing not just as clients; sometimes they play a provider role. In particular, UNICC, given its mandate and the nature of its activities, can be considered a cloud service provider for other United Nations organizations. This specific role is discussed in further detail in chapter V, on UNICC and system-wide cooperation. However, other organizations provide cloud services as well; an interesting case study on the provision of cloud services by the Universal Postal Union (UPU) to its stakeholders is included as annex I.

F. Previous work of the Joint Inspection Unit

27. JIU has never before conducted an in-depth review of the use of cloud computing in the United Nations system. However, in 2012, the Unit conducted a review of enterprise resource planning (ERP) systems in United Nations organizations (JIU/REP/2012/8). In the report, the Inspectors assessed the implementation, management and use of existing ERP systems. The Inspectors aimed, inter alia, to identify system-wide opportunities to share, harmonize and standardize ERP operations between the United Nations organizations.

28. The Inspectors noted that "[t]echnology constantly evolves, and new ERP software versions are released every four to five years. Organizations have the opportunity to enhance their ERP system and adopt new features and functionalities to meet changing business needs at each ERP upgrade. … Recent trends in the ERP industry include the development of cloud-based SaaS modules…" (ibid., paras. 124–125). The Inspectors also noted that ERP providers continued to develop their cloud-based services, which were already widely used in the private sector, and that third-party hosting solutions, including public cloud solutions, might raise confidentiality concerns to some organizations with regard to sensitive data (ibid., para. 126).

29. The Inspectors recommended the Secretary-General, in his capacity as Chairperson of the United Nations System Chief Executives Board for Coordination (CEB), to direct CEB to develop a common United Nations system policy regarding cloud-based solutions, before the end of 2014 (ibid., recommendation 4). In their joint comments, the United Nations system organizations supported this recommendation. Furthermore, "[s]ome agencies expressed enthusiasm for more aggressively exploring the use of cloud services, which they believed could promote greater flexibility, scalability and cost-effective options, including through a reduction in operating costs. In particular, agencies highlighted the benefits that a system-wide cloud policy would bring for ERP system strategies" (A/68/344/Add.1, para. 8).

30. Organizations urged that guidance on the handling of legal/regulatory constraints in terms of the storage of confidential intellectual property should be included in the guidelines for a common approach developed by the inter-agency mechanisms. The legal advisers of the organizations of the United Nations system had issued a statement on the employment of cloud computing services. While acknowledging the benefits of cloud computing as well as the risks, including the possible impact on the privileges and immunities of United Nations system organizations, they suggested that agencies take specific actions prior to initiating cloud services, including performing risk-benefit analysis and strengthening information classification policies and practices, evaluate in-house cloud services, such as utilizing UNICC, and ensure that decisions to utilize cloud services were taken at the highest institutional level (ibid., para. 9).

31. In a follow-up management letter (JIU/ML/2017/1), the Inspectors indicated that while the participating organizations had supported the recommendation, it remained neither accepted nor implemented. It should be noted that at the time of writing of the present review, the status of the recommendation remained unchanged.

32. The United Nations Secretariat, in its corporate response to the JIU management letter, indicated that the ERP Special Interest Group, the part of the Digital and Technology Network that worked on inter-agency collaboration in the context of ERP applications, had agreed to establish a group led by UNICC to develop a policy framework for ERP and cloud computing. Furthermore, according to the Secretariat, the next step was for all member organizations of the ERP Special Interest Group that had any cloud-related policies to forward them to UNICC for review and further discussion within the group. UNICC would convene virtual meetings to review the various policies and develop the policy framework. It was expected that the ERP Special Interest Group would review the outcome of the work in April and May 2018. However, no action has been taken since then and UNICC has not received any cloud-related policies to review. **The Inspectors remain convinced that a common United Nations system policy framework for ERP and cloud computing remains necessary and reaffirm the need to resume the implementation of the agreed course of action. In this regard, executive heads of United Nations system organizations that have any cloud-related policies should forward them to UNICC before the end of June 2020, in order to allow for the development by UNICC of a common United Nations system policy framework for ERP and cloud computing, to be finalized under the coordination of the Digital and Technology Network by June 2021.**

II. Current use of cloud computing by United Nations system organizations

A. Cloud computing: an everyday tool for different purposes

33. The United Nations system presently exhibits a full range of cloud adoption models and stages of development, and, consequently, different degrees of maturity. A small number of organizations do not use cloud computing at all, whereas others have ICT strategies that are strongly based on cloud services and resources, promoting a "cloud-first" approach. Examples of the latter include the United Nations Population Fund (UNFPA), the United Nations Entity for Gender Equality and the Empowerment of Women (UN-Women), the World Intellectual Property Organization (WIPO) and the International Labour Organization (ILO). Furthermore, WIPO, for example, established its Cloud Management Unit to manage and coordinate the use of cloud services, including management of the related contracts, for the organization's ICT projects. It provides assistance to programmes that need to deploy applications into the cloud.[12]

34. Ten organizations have indicated that they have specific cloud strategies and/or policies and guidelines in place, while six others include cloud guidance in their broader ICT strategies. At the time of writing of the present report, three organizations had indicated that their respective cloud strategies were under development or were being revised. Only four organizations have confirmed that they have no strategy in place for the internal use of cloud services: the World Tourism Organization (UNWTO), the World Meteorological Organization (WMO),[13] the United Nations Industrial Development Organization (UNIDO) and UPU. UPU is a paradoxical case, acting as a cloud service provider to postal operators as described in annex I, but lacking a cloud strategy for the internal use of cloud services. The Inspectors believe that cloud computing is a part of the broader digital context and, as such, cloud strategies should be an intrinsic element of a broader ICT framework. Some organizations refer to "cloud-first" strategies, while the United Nations Secretariat further elaborates, referring to a "cloud-first" but not "cloud-always" strategy, which gives priority to cloud-based solutions while recognizing that some special cases may require on-premises or more traditional approaches.[14]

35. A total of 22 organizations, constituting the vast majority of the organizations that answered the JIU corporate questionnaire, confirmed that they used various cloud computing solutions. Only two indicated that they did not use cloud-based services in a structured, planned and significant manner (UNIDO and UPU). However, even these organizations cannot guarantee that cloud computing, in any of its forms, is not used by their staff, given the ubiquitous availability, easy access and rapid growth of a wide offering of different cloud–based services, such as filing applications, survey tools and learning platforms.

36. The United Nations system organizations use cloud computing for different purposes, as follows:

(a) *Email and office productivity applications*. This general category of applications is currently the most representative and widespread use of cloud services, following a strong recent migration of these services to the public cloud by a number of organizations;

(b) *Business applications*. These are applications for various human resources functions, including talent management and online training, followed by customer relationship management and ERP system applications;

[12] WIPO, "Cloud hosting services policy: office instruction 15/2018", 25 May 2018.

[13] In its comments on the JIU draft report, WMO states the following: "… the use of cloud services is a major component of our IT strategy, in particular for managed desktop environment, document management and web-based applications for interacting with our Members. The choice between the use of cloud, SaaS or running our applications in hosted virtual environments is driven by cost, the need for business continuity and global access."

[14] "United Nations Secretariat cloud strategy" (April 2018), definitions, p. 7.

(c) *Websites (public and internal)*. Most organizations host their public-serving websites from the cloud for better global accessibility and separation from their internal computing resources. Some organizations also develop and serve their Internet websites from the cloud;

(d) *Application development*. Cloud-based application development environments are now increasingly replacing local, on-premises configurations;

(e) *Specialized applications*. A smaller number of surveyed organizations use ICT management and cybersecurity applications from the cloud, such as device management and software distribution, as well as threat detection and firewalls;

(f) *Hardware replacement*: for many ICT departments, replacing local computing hardware, storage and networking infrastructure with cloud-based infrastructure reduces complexity and the cost of operations. At the same time, this increases operational and technical flexibility due to the virtualized nature of cloud infrastructure.

B. Cloud computing: service and deployment models used in the United Nations system

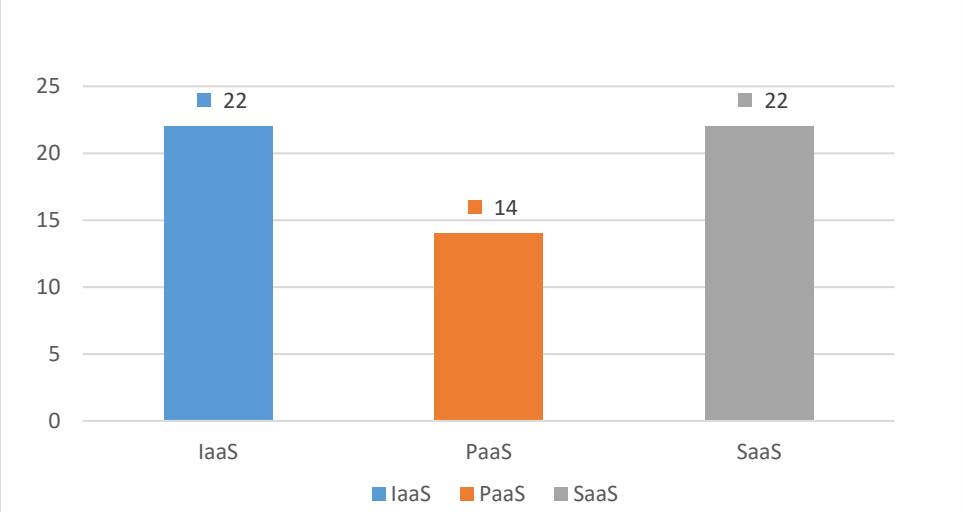
37. The following sections describe the cloud services and deployment models, as well as the main suppliers used by the organizations. In fact, cloud services, deployment models and suppliers are not independent and the organizations cannot freely choose any combination of these elements for a desired service. A choice of one of these elements – for example, a particular deployment model – may narrow down both logical and practical choices for the other elements. Annex II contains further information on the cloud services, deployment models, suppliers and products used by each participating organization that answered the JIU corporate questionnaire.

38. The most-used services models among respondents are IaaS and SaaS. These two service models correspond to the two major motivations that drive organizations towards cloud deployment: reducing the complexity of infrastructure and providing access to the innovative features of the most recent software applications offered primarily from the cloud.

39. As illustrated in figure V, PaaS is used by 14 organizations, out of the 22 that use cloud services. This service model is mostly used to develop websites, whether public or internal, as well as for the customization of applications.

Figure V
Cloud service models used by participating organizations

(Number of organizations)



40. All types of deployment and service models are used by United Nations organizations depending on the functionality demanded, as described in the following paragraphs.

1. Infrastructure as a Service

41. On one side, organizations wishing to reduce their dependence on and the complexity of hardware infrastructure are increasingly subscribing to the IaaS service model. The virtualization of their servers and their deployment in the cloud offers the following advantages:

(a) IaaS allows organizations to move their ICT infrastructure from traditional data centres to the cloud infrastructure with minimal technical changes. IaaS typically allows data and application servers to be virtualized and migrated to the cloud without the need to rewrite or purchase new software or significantly change its architecture;

(b) IaaS both allows and requires a high degree of control over the operating system and the supporting software infrastructure by the technical staff of the organization. This ownership of IaaS allows a significant degree of continuity of operations and reliance on a foundation of existing technical skills and capacities;

(c) Virtualized servers hosted in an IaaS environment relieve an organization from worries about the computing hardware, previously hosted in their local (or sometimes remote) data centres, and about the network infrastructure, connectivity and related power consumption;

(d) Virtualized services are easier to move from one physical server (or data centre) to another, and to back up and replace in case of hardware problems.

42. On the other hand, virtualized services, running in their own compartments on the providers' physical servers, share the hardware infrastructure with the services of other clients. In such circumstances, there may be some restrictions in terms of performance levels, which are assured through service-level agreements (SLAs). In normal circumstances, the security and privacy of a virtual service is not at risk in such shared environments. However, a certain minimal level of risk is inherent to the very architecture of IaaS.

43. The World Health Organization (WHO) utilizes all the major service models for their computing needs, among which are IaaS services by AWS. Virtual servers and storage resources located in the AWS cloud are used by WHO for hosting various web applications and their public website. Every visitor to the WHO public website is served by a web server running on a virtual machine somewhere in the AWS cloud.

2. Platform as a Service

44. Moving higher within the levels of abstraction of computing infrastructure, some organizations use PaaS to reduce the complexity of application development. PaaS services hide the complexity of the underlying infrastructure layers (hardware, operating system, networking, and auxiliary software), which are managed by the provider on the client's behalf, in order to allow the client to focus on the development of their customized applications. PaaS has the following features:

(a) It delivers online platforms for further software development or customization by the client, rather than being a ready-made product;

(b) It can be used to develop products that will themselves be used from the cloud, or it can be downloaded for deployment in a local network or private environment;

(c) PaaS platforms enable the development of a variety of products, from public websites or private websites (intranets), through customized software packages, and to mobile applications;

(d) In a PaaS environment, the cloud service provider is responsible for installing and applying the security updates for the operating system and all the software layers driving the development platform.

45. PaaS differs from IaaS in that the latter offers a much more basic layer or stack of computing services (networking, operating system, and so on) to the customers in a virtualized form, a layer that is hidden in PaaS. At the same time, PaaS differs from SaaS, because it does not offer the full final functionality for end users out of the box as SaaS products do. PaaS platforms have to be configured, customized or programmed– often

extensively – before they can be deployed in a production environment and offered to the end users of an organization.

46. SharePoint Online is an example of a PaaS service, provided by Microsoft. It is a web-based team collaboration platform, which enables organizations to create internal websites, document collections, information-sharing platforms and other similar solutions according to their needs. It can be considered as a set of building blocks for further customization and development towards an end product. The United Nations Development Programme (UNDP) uses SharePoint Online for building and running their internal websites. Other examples of PaaS services include ready-made platforms for building public websites.

3. Software as a Service

47. At the other end of the cloud spectrum, organizations subscribe to SaaS products to reduce the complexity of the entirety of their ICT operations, including related resources (hardware, operating system, networking and the software applications themselves). An example of an SaaS application is the Microsoft Office 365 suite,[15] including its email application, which is used by several United Nations organizations. SaaS has the following features:

(a) It offers a high-level of abstraction of ICT services: the client organization is practically an end user of an application that is hosted by a provider and is exposed only to the concrete application that is being used, and not to the underlying layers of supporting hardware, middleware and software supporting the execution of the application. In some cases, it is possible to have shared responsibility for very limited number of aspects of the infrastructure layers, but this is an exception rather than the norm;

(b) It reduces the complexity of setting up and maintaining an application for client organizations. It allows them to focus on its business features and the functionality desired, without having to worry about all the required technical work. A trusted and reputable provider will make sure that current industry standards and good practices are put in place for all their clients, which is sometimes difficult to maintain for small organizations;

(c) This very trend of standardization, while having mostly positive effects, necessarily constrains the client's ability to customize the application and its features beyond the flexibility that is (or is not) pre-built into the software application. Such constraints have both positive and negative effects: the negative side is the inability to customize the applications beyond the functionality offered by the provider, whereas this ability would enhance the effectiveness of the application for its use in certain cases by a particular organization; on the positive side, organizations are also prevented from undertaking customizations that are often too complex and too long, are difficult to maintain and bring low returns in terms of efficiency;

(d) A number of organizations – the Food and Agriculture Organization of the United Nations (FAO), UN-Women, WHO and WMO – indicated a strong preference for an SaaS-first strategy whenever possible, allowing them to avoid software development altogether for specific domains when they find a good enough solution among cloud applications available in the market.

48. As previously indicated, the choice of suppliers and the choice of service models are often linked: in addition to cost factors, most organizations choose suppliers because of their reputation, scale and guarantees offered, then adopt deployment models and service models that are available with these providers. Similarly, if an organization chooses an SaaS service model for a particular application, it will rarely be able to choose a deployment model for this service, given that SaaS services tend to be highly standardized in order to achieve benefits of scale.

[15] Office 365 is a cloud-based subscription service from Microsoft that brings together applications such as Excel and Outlook with cloud services such as OneDrive for filing and Microsoft Teams as a collaboration tool. Office 365 allows anyone to create documents and share them from anywhere on any device.

49. Another constraint that guides the choice of both service model and deployment model, particularly for business applications delivered as SaaS, is the fact that providers are now, in a sense, forcing their clients to move to the cloud by launching new features on a cloud-first or even cloud-only basis. For example, the United Nations Educational, Scientific and Cultural Organization (UNESCO) noted that human resources management solutions were not available at the same level on premises, since the solutions offered by the leading providers were all SaaS. Similarly, UN-Women, for example, cited the availability of better products and services as their main reason for using cloud services.

50. The United Nations Secretariat cloud strategy proposes a hybrid, multi-cloud approach. An on-premises private cloud allows for easy integration of internally hosted systems (such as legacy applications[16]) while third-party, public cloud technologies host an increasing number of enterprise systems and platforms. The Secretariat makes use of multiple third-party providers in order to leverage specific features and services and ensure continuity of operations.[17]

C. Cloud-based enterprise resource planning systems

51. ERP systems offer many potential benefits. Fundamentally, they are information systems that offer a modular and comprehensive set of functionalities (such as finance and accounting, human resources management and supply chain management), facilitating the broad management of organizations and enabling organizations to integrate their own data into the built-in business processes of a unified, or standardized, information system. Their modular design allows the selection of the specific functional applications that are most relevant to the needs of an organization.

52. Organizations deploying ERP systems today have three deployment models to choose from: on-premises, hosted or cloud-based. Security in the cloud has been one of the main concerns preventing organizations from adopting cloud-based ERP applications. Applications, particularly mission-critical ones, cannot simply be migrated to cloud service providers as if it was simply a new hosting facility. ERP applications are particularly at risk given the nature of their functions, in areas such as human resources and payroll. As with all new technologies, there are new challenges associated with cloud-based ERP applications, and potentially even an increase in their vulnerability. However, in the past five years, there has been a marked improvement in cloud security. Moreover, as technologies continue to mature, organizations rely on the cloud service provider to implement better security measures than they would have otherwise used on their own premises.[18]

53. Cloud-based ERP solutions are gaining momentum, with market-size projections calculated at between $25 billion and $30 billion over the next five years. From a strategic perspective, cloud-based ERP deployments are promising because of their simplicity and their lower cost of ownership over conventional on-premises and hosted ERP solutions.[19] In addition to the traditional ERP vendors, new providers (such as Salesforce and Workday, among others) are already having an impact on the ERP market by offering advanced, flexible, highly mobile and easy-to-use applications in diverse functional areas, including finance, procurement, supply chain, marketing, sales and human resources. Sold on a subscription basis, these SaaS systems offer clients the promise of reduced costs, among other advantages. The product of integration of these applications with legacy ERP systems is known as “hybrid ERP”.

54. Cloud-based ERP systems are an interesting alternative for new organizations, given the flexibility offered and lower initial capital investments required. Thus, entities such as the Green Climate Fund, UNFPA, UN-Women and others have focused their ICT strategy

[16] A legacy application (“legacy app”) is a software program that is outdated or obsolete. Although it still works, it may be unstable because of compatibility issues with current operating systems, browsers and information technology infrastructures. See https://searchitoperations.techtarget.com/definition/legacy-application.

[17] “United Nations Secretariat cloud strategy” (April 2018), p. 2.

[18] Cloud Security Alliance, “State of enterprise resource planning security in the cloud” (2018), p. 9.

[19] Ibid., p. 8.

on cloud-based systems, in particular SaaS applications, which provide some of the functionalities contained in ERP systems. It is to be noted that only ILO, UNDP and UN-Women have already moved some parts of their ERP systems to the cloud (in the case of ILO, its financial processing and reporting); the aspects in question can be considered medium complexity services that require some additional planning and migration efforts. However, only the Pan American Health Organization (PAHO) has moved all of its ERP to the cloud, requiring services that are more complex.

55. PAHO is the first organization in the United Nations system to have implemented a more comprehensive cloud-based ERP solution – the Pan American Sanitary Bureau Management Information System (PMIS)[20] – driven, inter alia, by modernization and the need to renew its ageing legacy management information systems. Based on a system provided by Workday, PMIS was implemented between 2015 and 2016, and, according to PAHO, on time and within budget. Box 5 contains a synthesis of the major elements of a case study that was conducted into the reasons behind and implementation of the PAHO solution, including lessons learned.[21]

Box 5

The experience of the Pan American Health Organization

Various considerations drove the preference of PAHO for a cloud-based ERP solution. Functionally, cloud-based systems tend to have better mobile interfaces than traditional systems, allowing users to perform tasks on tablets and smartphones. This consideration was especially important given the decision by PAHO to make system use compulsory for staff, regardless of role and location. The cloud-based option was judged safer than an on-premises system, due to the backup structures and security protocols that cloud-based systems use to prevent data loss. Access to PMIS by PAHO personnel, including through mobile devices, in post-disaster or emergency situations was also an important consideration. Accurate calculation of PMIS maintenance and upgrade costs, and the ability to re-configure the system to meet the changing needs of staff and managers, were fundamental to the system selection made by PAHO.

This new system represented a rather abrupt move from a legacy world of specified functionality to more limited PMIS business process configurations, with a much broader user base. PAHO applied a four-point plan to promote PMIS-related organizational change and a shift in mindset, by explaining: (a) why the change was needed; (b) the implications for programmatic activities; (c) the available tools to support continuous change; and (d) the effects on accountability, responsibilities and PMIS governance.

While the preferred solution has met the needs of PAHO, it has also posed new and sometimes unexpected change management challenges. The reliance on standardized systems highlighted the opportunity that SaaS cloud-based systems offered for driving through essential re-engineering or streamlining of processes. The inability to customize the cloud-based PMIS system had the unanticipated benefit of forcing a clean-up of the enabling policy and procedures environment, resulting in the establishment of policies that are clearly linked to (new) implementing standard operating procedures.

The main constraint reported in the case study, is that PAHO was forced to adapt its procedures to match the options of the specific PMIS applications. This has come with additional costs necessary to adapt many existing procedures, and to continually monitor and manage PMIS system enhancements. Updates are released in the cloud by the vendor weekly and every six months through larger software functionality upgrades, thus requiring continuous change and change management of PAHO work practices. Frequent system reconfigurations and automatic upgrades pose a hidden cost by consuming PAHO staff time and requiring retraining.

[20] The Pan American Sanitary Bureau is the executive arm of PAHO.

[21] United Nations System Staff College, “A cloud-based ERP renovates work practices and changes behaviour at PAHO: mini case study #2/2017” (2017).

56. As is the case when considering any cloud solution, organizations must think through those ERP security challenges and, given the strategic nature of ERP systems in particular, undertake a comprehensive risk analysis, establishing appropriate contingency plans and risk mitigation measures, including exit strategies when deciding on the implementation and/or migration of their ERP solutions to the cloud.

D. Expected benefits of cloud computing

57. The analysis of the answers provided by participating organizations in response to the JIU corporate questionnaire indicates that their essential reasons for using cloud computing services often coincide with the theoretical core cloud benefits, which are well defined in literature, emphatically promoted by vendors and briefly introduced in the present report in the description of the different cloud service and deployment models (chap. II). Among those benefits, the in-built ability to dynamically supply the computing resources required according to changing needs is the primary reason why organizations decide to use cloud computing. While scalability and elasticity are slightly different, the terms are often used interchangeably in relation to cloud services. Both are expected to lead to efficient cost management, where charges are related to the resources actually used over a period of time. A considerable number of organizations (13) cited elasticity, scalability or both as one of their main reasons for using cloud computing.

58. The following paragraphs explore other common benefits provided by cloud computing. In broad terms, the reasons and benefits mentioned by organizations are diverse in nature – technical, financial and functional – but these divisions are often blurred. Technical advantages often enable other benefits, such as collaboration or agility.

1. Wide global access

59. Most of the United Nations organizations have a significant presence worldwide, with multiple field offices and geographically dispersed teams requiring efficient communications, coordination and collaboration. While some of that communication still takes place through dedicated private networks, the public Internet infrastructure increasingly plays an important role in enabling global connectivity.

60. Cloud-based services typically benefit from being connected via major Internet pipelines and ever-expanding internal networks. They are also designed and built for delivery through the public Internet and worldwide access. Additionally, large cloud providers seamlessly use a number of techniques to ensure fast access to the services that they offer from different locations around the globe. Cloud-based services seem to offer an advantage in terms of enabling global access to services and for the interconnectivity of geographically dispersed teams.

61. The United Nations Office for Project Services (UNOPS), for example, indicated that its “current ICT infrastructure does not support the needs of the organization in terms of application resilience, accessibility and collaboration across geographical locations and networks. UNOPS is a global organization with staff in most areas of the globe. We need to be able to deliver fast application experiences across the globe. A single data centre location ... is not enough.” Other respondent organizations that list global access as one of the reasons for using cloud services are ICAO, the Office of the United Nations High Commissioner for Refugees (UNHCR), UNDP, the United Nations Relief and Works Agency for Palestine Refugees in the Near East (UNRWA), UN-Women and WHO.

62. Major cloud service providers operate globally and are continuing to invest in an effort to offer better coverage for their cloud services. Although the leading public cloud providers, AWS and Microsoft Azure, both offer core IaaS features such as virtual machines, storage and databases, they take very different approaches in offering cloud services, including at the most basic level of how their data centres are constructed and positioned around the world. The AWS cloud spans 60 availability zones within 20 geographical regions around the world, with plans announced for more, while Microsoft has 54 regions available in 140 countries worldwide. However, those numbers cannot be compared directly. While AWS uses availability zones as the basis for its cloud, with each region made up of at least two zones,

Microsoft instead uses regions only and does not guarantee that each region will have multiple data centres.

2. Service continuity

63. Linked to the wide geographical availability of cloud services, the high level of ICT service continuity, also known as "business continuity", is one of the most appreciated properties of cloud computing for organizations and is often a major reason for moving their operations to the cloud. Ensuring the availability of data and systems is an important part of ICT security. Whether an organization is experiencing a natural disaster, power failure or other crisis, having critical data stored in the cloud isolates them from adverse conditions at the organization's location. Being able to access these data quickly allows that organization to conduct business as usual, minimizing any downtime and loss of productivity.

64. The amount and widespread availability of ICT resources offered by the data centres of the major cloud service providers allow for redundant facilities, multiple backup locations and worldwide support and systems 24 hours a day and seven days a week, facilitating business continuity in a manner that cannot be matched by United Nations organizations using their own resources, even if these resources could be pooled. This is confirmed by the answers provided by the organizations that responded to the JIU corporate questionnaire, which show a clear perception that higher service continuity is easier to achieve in the cloud environment than using on-premises data centres. Although the exact modalities differ, half of the respondents indicated that the cloud played a role in their business continuity planning and implementation.

65. The corporate responses received indicated that only three organizations – the International Atomic Energy Agency (IAEA), the United Nations Environment Programme (UNEP) and WHO – encountered challenges in relation to service continuity. UN-Women indicated that over the four years that its email services had been fully hosted by Microsoft, it had experienced total downtime of less than four hours, and that it was unlikely that any other vendor could have delivered uptime anywhere near that level for the same price.

66. However, it should be noted that where specific responses were received, a relatively high number of organizations (nine), about a third of responses received, showed an exclusive reliance on the vendor's disaster recovery mechanisms for the organization's service continuity. For example, UN-Women indicated that while it had disaster recovery and business continuity plans in place, the plans relied on cloud vendors to deliver on contractual obligations. At present, this reliance does not pose practical problems because most of cloud-based solutions used by United Nations organizations are SaaS applications and not mission-critical or strategic. However, it does raise questions of long-term sustainability. Disaster recovery and business continuity plans should anticipate cases in which the selected cloud service providers go out of business. Looking back at the history of the ICT and Internet industries, there are significant examples of large-scale services and providers that dominated markets at one time, only to decline or discontinue after a number of years. The reasons for this have ranged from rapid technological innovation often leading to obsolescence – particularly significant in the ICT world – to a voluntary change of major market actors' focus towards higher-profit segments of the market. **While the current domination of the cloud market by a small number of very large vendors is unprecedented, the "too big to fail" paradigm has consistently proven wrong. Consequently, scenarios in which these main vendors and their services lose their advantages or reliability should not be completely excluded from the long-term strategic thinking required by the United Nations system.**

Recommendation 1

The executive heads of the United Nations organizations should ensure that business continuity planning includes strategies and measures to mitigate the risk of failure by cloud service providers to deliver the contracted services.

3. Cost benefits

67. Cost-efficiency is one of the main promises of cloud computing technology. Cloud suppliers justify this claim on the basis of the fact that computing resources are shared among clients, and the economies of scale resulting from large data centres while each client is billed for their actual use of resources. Additionally, using public cloud services eliminates the capital investments required to purchase computing hardware, software and associated networking infrastructure.

68. While much focus is placed on cost savings as one of the most relevant benefits of cloud computing, much of those savings are difficult to quantify. Cloud computing might indeed enable organizations to avoid future costs. For example, the implementation of scalable infrastructure can reduce future capacity costs, and the faster development of applications can reduce development costs. However, these costs do not reduce the current ICT budget, and some costs are sometimes hidden or overlooked.[22]

69. A considerable number of respondent organizations mention cost savings as one of the main reasons for using cloud computing. However, most of them do not elaborate more specifically how these estimated savings actually resulted from the use of cloud computing, assuming this is self-evident. Other organizations are more specific in their responses. For example, ILO and UNDP cite lower start-up costs (no capital investment) and lower cost of ownership among the main reasons for the use of cloud services.

70. The World Food Programme (WFP) indicated in its response that cloud services provide value for money. UNDP also included "efficient expense management due to the elastic nature of resources" in their response, referring to one of the key properties of cloud computing. FAO provided an interesting viewpoint, stating that cloud computing enabled the transformation of fixed and hidden costs into clear variable costs, and payment according to use. This statement clearly reflects the difference between (a) the traditional computing model, which results in complex cost calculations that include capital investment in hardware, facility costs, human resources, licences and so on, and (b) the cloud billing paradigm of computing as a utility. Moving to cloud computing may reduce the cost of managing and maintaining ICT systems. Cloud services are typically "pay-as-you-go", or paid on demand, which allows end users to utilize computing resources as needed. Cloud computing maximizes the utilization of computing resources and reduces the operation and maintenance costs, especially during off-peak times. In addition to reduced acquisition costs, agencies may also be able to reduce ICT operating expenses by avoiding the cost of system upgrades, if new hardware and software is included in the cloud contractual agreement. Additionally, the overall staff allocation is smaller, and energy consumption costs may be reduced.

4. Security benefits

71. With the global growth of Internet usage, cyber threats and incidents are increasingly frequent. In recent years, there has been a growing number of high-profile data leaks, intrusions, hijacking and other forms of cyber incidents globally, across all sectors and domains. United Nations organizations are high-profile targets and they are aware of the trend.

72. For some of organizations, security is one of the main reasons for using cloud computing. Five organizations listed better data security as part of their motivation for cloud adoption. At the same time, there are organizations that consider data security as one of the main challenges of using cloud computing services. Three organizations explicitly listed cloud data security as a challenge.

73. Organizations in favour of cloud-assured security consider that cloud providers are better placed to organize and maintain security in the ever-changing threat landscape than in-house ICT departments. According to this reasoning, cloud providers benefit from advantages of scale and volume, which allows them to finance the investment into technical and human capacities for better cybersecurity. Some of the respondent organizations (WIPO,

[22] World Bank, "Cloud computing overview", June 2016, p. 20.

for example) consider that only the biggest public cloud providers (such as Microsoft, Google and Amazon) can provide adequate ICT security today.

74. On the other hand, relying on a third-party external cloud service provider already creates a new risk and the very limited number of dominant cloud suppliers leads to a high concentration of data from the United Nations system in a small number of commercial data centres. A recent wave of high-profile data leaks and breaches hitting the biggest Internet companies – for example, Amazon in November 2018, Google in October 2018 and Facebook in September 2018 – shows that they are vulnerable. Paradoxically, many of their cloud users may be experiencing a somewhat false sense of safety. Given that cybersecurity is often mystified in the media and by vendors, it is clear that it is not easy to make a balanced evaluation of security criteria for any organization.

75. Moreover, the large commercial providers do not necessarily cater for the security specifics of the United Nations system and are not in a position to take full advantage of the range of possibilities offered by United Nations organizations. Information-sharing and collaboration are today considered as one of the key elements of detecting and preventing cyber threats. On the other hand, commercial vendors face a delicate balance between protecting resources, skills and information for their own competitive advantage and sharing them for the benefit of wider national or international safety.

76. Exploring complementary and alternative approaches jointly could help United Nations organizations build more comprehensive and nuanced security for the cloud, while avoiding some shortcomings resulting from overreliance on the largest public cloud vendors. Cloud computing enables cloud-based security, which in itself is advantageous over the traditional on-premises model. It can be less expensive, more efficient and easier to manage since it allows for centralized policies, and it can provide a higher level of security as it is proactively managed by a team of security experts. An advantage of a cloud-based security solution is that the United Nations can gain the ability to centralize security policies and rules.

77. Efforts by UNICC to strengthen and grow security services, and particularly its efforts to combine purely technical measures with "softer" aspects of collaboration and information- and experience-sharing, support a community approach among its client/member organizations. They constitute a step in the direction of providing security services tailored to the needs of the United Nations system. More details on UNICC services are given in the chapter V.

78. UPU is one of the respondent organizations that, by designing and delivering their own cloud services to their member countries, considered and adopted a customized approach to cloud security while also using UNICC support. UPU took a conscious decision not to use the cloud infrastructure of the largest commercial cloud providers, such as Amazon or Google. Their decision was to locate the infrastructure and the data that it hosts in Switzerland, under a jurisdiction that fully respects United Nations privileges and immunities, and to work with a local communications provider despite its small size compared with the leading global vendors. It considers the network accessibility, security and protection offered through this provider to be adequate for the needs of the specific system that it operates. More details on the approach of UPU is given in annex I.

5. Flexibility and agility

79. Most cloud products are preconfigured, tested and designed to be quick and easy to deploy. Clients can normally select the products and operating parameters online through a user-friendly interface, and the service is available for use almost instantly. This is in stark contrast to the lengthy deployment of conventional computing resources and it is rightly perceived as adding significant agility to an ICT environment. The downside of this approach is an apparent lack of flexibility and customization scope in standardized, ready-made cloud products.

80. Some organizations – for example, UNHCR, the United Nations Children's Fund (UNICEF), the United Nations Secretariat and WIPO – include agility explicitly as one of the main reasons for using cloud computing. A few other responses that use different wording could also be counted under this category of benefits. IAEA, for example, referred to "faster deployment". Cloud computing allows the faster development of applications: for many

Governments and organizations, it can take weeks, if not longer, to order new servers, set them up, and then build a new application. Other responses stressed the outcome of keeping up with the changing needs of the organization as a benefit (WFP), which can be directly linked to agility.

6. Facilitation of innovation

81. Due to their ability to dedicate significant resources to research and development, large cloud providers are typically able to use and offer recent and innovative products and technology, at a pace that would be difficult to follow for ICT departments of individual organizations. Smaller, specialized providers are also able to offer innovative services in their niche markets.

82. Many new digital technologies and products, such as artificial intelligence, blockchain or big data analytics, are promptly offered as cloud services by companies such as IBM, Microsoft and Google, which makes it easy for cloud users to experiment and build applications based on these services. ICAO, for example, in its response, referred to leveraging innovative tools such as artificial intelligence as one of their main reasons for using cloud services.

83. However, access to cloud and its innovative service benefits or features does not guarantee that the client organizations will automatically be innovative. This point is recognized in some of the responses. The United Nations Secretariat referred to innovation opportunities while FAO mentioned an increase in innovation capability, both recognizing that innovation is a possibility that needs to be realized by the client.

84. Six organizations included innovation, in some form, as one of the main reasons for using the cloud services (FAO, ICAO, UNICEF, the United Nations Secretariat, UNOPS and WHO), while two explicitly listed ICT modernization (ICAO and UNIDO).

7. Modernization of information and communications technology

85. A few organizations listed modernization, a related concept, as one of their reasons for using cloud services. Cloud technologies may offer a solution for the replacement of obsolete ICT systems. While this benefit may be difficult to quantify, cloud computing can play an important motivational role and be a factor of productive consolidation of organizational ICT.

86. However, the Inspectors would like to highlight that before embarking on a modernization project based on cloud computing, organizations should undertake a careful analysis of their current infrastructure. As noted by the Information Security Special Interest Group, an inter-agency group formed by ICT experts, if the current network infrastructure is unreliable or is already highly utilized, then moving to the cloud may be too much of a burden on the existing infrastructure. In such situations, either the network infrastructure must be upgraded before considering a move to a public or hybrid cloud or, alternatively, a private cloud on a dedicated line should be considered.[23] This is further confirmed by FAO in its corporate answer, in which it indicated that the new cloud-based model, based on centralized services, required more robust connectivity (network infrastructure to access the Internet), especially for the public cloud, and that a revision of the network model (dynamic bandwidth versus fixed bandwidth) was ongoing although time was required to deploy the new solutions.

87. There are some risks related to the desire to modernize organizations' ICT infrastructure. Marketing campaigns by commercial providers sometimes make it difficult to assess the true innovative dimension of new products and services, or their appropriateness for the situation of a given organization. This could lead to increased spending on solutions that do not provide proportional benefits. It is also worth noting that innovative products can fail to become industry standards in medium or long term.

88. Another aspect of modernization is related not only to the ICT infrastructure used by an organization, but also to the staff skill set available. In-house ICT skills gaps are often a

[23] Information Security Special Interest Group, "Use of cloud computing in the United Nations system", p. 17.

hurdle for innovation and modernization within organizations. At least one organization (ILO) explicitly referred to the lack of in-house skills as a reason for opting for cloud-based computing services. A number of others cited a similar motivation, referring to access to best practices and higher industry standards by deploying cloud-based services, with the implication that more effort and a skill upgrade for their in-house operations would otherwise be required.

8. In-built functions and feature benefits

89. According to a number of responding organizations, certain cloud-based products offer features that are available only with a cloud version of an application or service and not through the traditional distribution channels with local installation and ownership of applications and services. Software and service providers proposedly introduce such features in order to discourage or discontinue the purchase of traditional versions of their products and attract the clients to cloud-based editions. This trend will most likely continue to gain in importance and will have an impact on future procurement decisions.

90. UNESCO observed that human resources management solutions were not available at the same level on premises, since the solutions offered by the leading providers were all SAAS, and many of the (future) functionalities were or would not be available as many vendors focused on cloud solutions and actively encouraged the move to the cloud. It also observed that although the on-premises solution was more cost-effective, it was decided to use the cloud version as it was richer in functionality and recommended by all potential implementation partners.

91. Other respondents listed similar reasons for choosing cloud-based services. The International Trade Centre (ITC) stated that some features of the product and services were only available as cloud options. UN-Women listed “Availability of better products and services” and referred to value added in the form of new features automatically available as well as new add-on features or services.

92. Similarly, to innovation and modernization benefits, combined with the reported functional advantage of cloud-based products, some organizations mentioned the idea of future-proofing their ICT resources using cloud computing services. With frequent updates, especially in the SaaS segment, and priority given to the cloud-based versions by vendors, the organizations see the cloud option as secured against obsolescence, which self-hosted installations can suffer.

III. Cloud computing: risks and challenges

93. Cloud computing offers many benefits, as already indicated, but it also comes with risks. One key feature of cloud computing is that remote data centres host applications and data and replicate them across multiple locations worldwide. Some of the risks associated with cloud computing are thus the same as those inherent to traditional ICT systems that use remote and distributed processing, with data and information travelling through broadband networks and/or the Internet, as well as those associated with outsourced service provisioning, whereby one or several third-party actors intervene, requiring additional security precautions.

94. The challenges associated with cloud computing are also related to confidentiality issues with regard to sensitive or private data. It should be noted that risks can be mitigated, or some aspects of risk can be transferred partially to the cloud service provider, by ensuring clear contractual safeguards, but there will always be a residual risk. Organizations dealing with significant amounts of sensitive information may therefore decide to limit the use of certain cloud-based solutions to systems handling only unclassified content. In fact, this is the case for several organizations that decided not to use cloud computing solutions to process or store confidential data.

95. The United Nations organizations are well aware of the specific risks associated with cloud computing, as confirmed by answers provided to the JIU corporate questionnaire and the interviews held by the Inspectors. Moreover, the Information Security Special Interest Group analysed cloud computing risks and made recommendations on risk mitigation, concluding that United Nations agencies should conduct their own, context-specific risk analysis.[24] **As the business and regulatory frameworks change and new risks arise, risk assessments should be a regular activity and a key mandatory step in any consideration of cloud computing solutions.** It should be noted that, in most cases, no specific resources are assigned for risk assessments. In the view of the Inspectors, it might be advisable to allocate a dedicated budget for this purpose.

96. The following paragraphs contain an overview of the challenges that organizations noted in their responses to the corporate questionnaire. While no major problems were reported, migration to cloud computing is not without challenges. The responses show a wide variety of approaches and levels of awareness among the organizations. However, a basic level of risk awareness exists across the system, and the organizations clearly identified the main risks introduced by cloud computing. The following synthesis may facilitate the sharing of useful experiences and provide a broader perspective on the challenges of cloud deployment.

A. Potential loss of governance of information and communications technology

97. ICT governance questions deal with the management of technology as opposed to the technology itself. [25] A governance mechanism is required, inter alia, to ensure that the benefits of cloud computing are realized, but also that expectations are effectively set and managed. There is a potential loss, or reduced effectiveness, of governance as agencies may cede control to cloud service providers on a number of issues that may impact their security. Loss of control may lead to the inability to comply with security requirements, a lack of confidentiality, integrity and availability of data, a deterioration in performance and quality of service, and the introduction of compliance challenges.[26]

[24] Information Security Special Interest Group, “Use of cloud computing in the United Nations system”, p. 5.

[25] ICT governance is defined as a system that ensures that the appropriate structure and levels of decision-making, supervision, monitoring and control are in place to guarantee the appropriate use of ICT resources in support of the mission, or strategic goals, of the organization.

[26] Information Security Special Interest Group, “Use of cloud computing in the United Nations system”, p. 6.

98. Governance can be structured in accordance with internationally accepted standards for ICT governance such as Control Objectives for Information and Related Technology (COBIT) 5.[27]

B. New security requirements

99. The multi-tenancy nature of cloud computing, remote access to cloud computing services and the number of entities involved pose security risks. However, many of these risks can be mitigated with the application of traditional security processes and mechanisms. As with any technology, security risks and challenges need to be managed and overcome. Security considerations range from general and traditional security concerns, such as the physical security of ICT infrastructure or end user authentication, to issues specific to the cloud service and deployment models being adopted. The cloud service model will drive the responsibilities and ownership of some of the key characteristics of business-critical applications, while the selection of a specific deployment model (private or public) will determine the need for specific and additional security requirements.

100. Furthermore, ITU through the study groups of the ITU Telecommunication Standardization Sector (ITU-T) develops international standards known as ITU-T recommendations, including relevant recommendations for enhanced cloud security. The World Telecommunication Standardization Assembly meets every four years to establish the topics for study by the ITU-T study groups, which are formed by ICT experts from all over the world, including from the private sector. Issued in 2015, recommendation ITU-T X.1601 (10/2015) contains a security framework for cloud computing, in which security threats and challenges in the cloud computing environment are analysed and a framework methodology provided for determining which security capabilities require mitigating security threats and addressing security challenges.[28] The ITU-T study groups are open to the participation of interested actors. **The Inspectors would like to encourage the United Nations organizations to actively participate in the development of relevant ICT standards, including those related to cloud computing, by participating in the ITU-T study groups in accordance with the ITU legal framework.**

101. The section on the expected benefits of cloud computing (chap. II, sect. D) indicates that some organizations consider that cloud services can ensure a higher level of cybersecurity for their ICT operations, while other organizations consider that security risks are higher in the cloud than on-premises operations. The two differing perspectives reflect the complexity of the cybersecurity issue. In the present section, different security aspects of cloud computing will be considered, beyond the issues of data confidentiality and privileges and immunities discussed later in the report.

102. In considering security challenges, it should be noted that different organizations often have different operational needs, as well as different risk appetites. One reason for their differing needs is that their digital assets have different levels of sensitivity. This does not mean that data owned by some organizations is more valuable than those held by others, but only that the damage caused by the misuse of data can have more devastating effects on the image and safety of a particular organization's operations or the people affected. For example, a leak of data containing refugees' personal details or location may have more dangerous consequences than a leak of data containing atmospheric measurements. When

[27] COBIT is a set of best practices for ICT management developed by the Information Systems Audit and Control Association (ISACA) and its IT Governance Institute. Some other examples of international standards are "Information technology: governance of IT for the organization", ISO/IEC 38500:2015; the Capability Maturity Model; and "Information technology: service management", ISO/IEC 20000 series.

[28] Other ITU-T recommendations relevant to cloud computing are the following: recommendations X.1602–X.1639 on cloud computing security design; recommendations X.1640–X.1659 on cloud computing security best practices and guidelines; recommendations X.1660–X.1679 on cloud computing security implementation; and recommendations X.1680–X.1699 on other cloud computing security issues. For further ITU-T recommendations relevant to cloud computing, see www.itu.int/itu-t/recommendations/index.aspx?ser=X

highly sensitive data and additional layers of control and encryption are needed, extra protective measures may make cloud solutions expensive and, in those cases, potentially unworkable.

103. Besides differing needs, organizations also show differing levels of risk tolerance. An acceptable risk to one organization is often not acceptable to another. This may be affected by an objective risk analysis or data sensibility previously mentioned, but it also reflects subjective aspects of an organizational culture.

104. Only three organizations mentioned security as a challenge or concern in their questionnaire responses. None of these responses indicate a major concern, nor do they share any reports of past security incidents, which is not an indication that such incidents did not happen. Overall, the questionnaire responses can be taken as an encouraging sign of a relatively smooth cloud security experience so far. In addition, UNOPS, for example, in its response, reiterated the belief that the cloud was a safer place for its computing workloads.

105. Additional information collected during the interviews and meetings suggests that there are both benefits and challenges that were not reflected in the questionnaire responses but help construct a broader picture of the security aspect of cloud computing in the United Nations system.

106. Small and medium-sized organizations often have limited resources, both human and budgetary, for implementing the appropriate levels of cybersecurity within their on-premises data centres. For them, using cloud-based services may be a way to benefit from resource pooling, implement industry's best practices and share the burden of demanding and complex cybersecurity measures at an acceptable cost. Some vendors even claim that their cloud version of a product is safer than versions that they offer for self-hosting (such as Microsoft with reference to its Active Directory services), which is an additional argument in favour of a secure cloud environment. On the other hand, using cloud services increases the exposure of organization's data and applications. Some of the smaller organizations have registered a sharp increase in phishing attacks since their migration to cloud-based Office 365 applications.

107. Further security risks may occur with business units, or individual users within an organization, deploying cloud-based solutions without enough coordination with their respective ICT units and without sufficient regard for security measures. Sometimes staff members, individually and spontaneously, subscribe to cloud services that address their immediate needs without knowing that these services, widely available, are cloud-based, such as SurveyMonkey for the purposes of conducting surveys, Dropbox for file-sharing, and social media networks. Cloud-based file-sharing is one of the first services that users seek. Organizations have identified this risk and some regulate the use of these cloud services through relevant internal policies.

108. UNESCO, for example, concluded in its risk assessment that it would be better to have cloud solutions offered by its central ICT unit than to have cloud services used by staff individually. Similarly, UNWTO identified a need for cloud-based file-sharing and implemented an organization-wide solution to prevent the loss and/or uncontrolled use of organizational data.

109. **The Inspectors would like to advise United Nations organizations that have not yet done so to include relevant provisions in their respective ICT and/or cloud strategies to prevent the uncoordinated use of cloud services by organizational units and/or individual staff members.** In those cases, where relevant policies do not exist, or in doubtful cases, prior clearance from the respective ICT units should be sought before allowing the use of any cloud service by either individual staff members or business units.

110. Another risk is that simply by moving their computing to one of the large, reputable clouds, organizations may develop a false sense of security. This is especially the case if the move is not accompanied by a number of architectural and operational checks and changes (especially for IaaS and PaaS), in order to avoid creating weak and vulnerable links in the technology chain and benefit fully from the security of the cloud provider. From the examples and the discussion above, it is clear that security in the cloud is a complex issue, with no one-size-fits-all solution. There are some inherent security risks specific to the cloud environment,

which can be assessed, managed and deemed acceptable for several use cases and organizations. There are also security advantages in the cloud for certain use cases, such as for agencies operating in geographically dangerous locations. Like on-premises data centres, cloud environments can be made more secure or less secure by clients' and vendors' choices. The public cloud offerings of the biggest providers, which currently host the majority of United Nations system's data, are not the only option, and the organizations could be looking at complementary options to reduce strategic risks for the United Nations community as a whole. UNICC security services can be an alternative to consider in this regard, as discussed chapter V.

111. An additional new security risk is related to the cloud service provider's personnel. With cloud computing, in-house ICT teams are not the only ones managing the new services. The Information Security Special Interest Group has asserted that for this reason, organizations must clearly define roles for managing cloud vendor relationships and service delivery. In the Group's view, one key aspect of an agency's due diligence, and a key control to implement, is ensuring that the cloud computing provider hires people that are trustworthy, and United Nations agencies should ensure that the cloud provider has policies in place to screen all candidates for employment and ensure that detailed reference checks are conducted, especially for sensitive jobs. **While the Inspectors agree with the Group's assertion, they call for a unified approach across the United Nations system, as it is simply unrealistic to expect each organization to be able to efficiently address individually the issue of the trustworthiness of the cloud service providers' personnel who deal with security and sensitive data. A collective stand will enhance the negotiating power of the United Nations organizations and may be conducive to better contractual terms, in particular when dealing with the same main cloud service providers.**

112. The Government of the United States of America provides good examples of different security requirements managed within a single framework, including the Federal Risk and Authorization Management Program (FedRAMP), the Department of Defense Cloud Computing Security Requirements Guide, [29] the Criminal Justice Information Services Security Policy,[30] and the International Traffic in Arms Regulations.

113. Major cloud service providers now offer specific products – such as Microsoft Azure Government or AWS Cloud for Government – that comply with the functional and security requirements demanded by FedRAMP. For example, Microsoft Azure Government provides hybrid flexibility, deep security and broad compliance coverage across regulatory standards. The key difference between Microsoft Azure and Microsoft Azure Government is that Azure Government is a sovereign cloud. It is a physically separate product that is dedicated to United States Government workloads only, built exclusively for government agencies and their solution providers. Azure Government is designed for highly sensitive data, enabling government customers to transfer mission-critical workloads to the cloud safely.

114. **The Inspectors believe that United Nations organizations should develop a joint approach to cloud security services, establishing a set of common basic requirements to be implemented across the United Nations system and encourage the sharing of relevant requirements and knowledge to support the creation of common best practices.**

C. Vendor lock-in

115. Whether the decision is to build a private cloud or to go to a public cloud, there will always be a certain degree of vendor lock-in. The degree of lock-in varies, particularly when it comes to deciding to move out of a public cloud or when using proprietary solutions that make migration, portability and integration more difficult.

[29] The Cloud Computing Security Requirements Guide defines the baseline security requirements for cloud service providers that host the Department's information, systems and applications.

[30] Law enforcement and other government agencies in the United States must ensure that their use of cloud services for the transmission, storage or processing of relevant data complies with the Criminal Justice Information Services Security Policy.

116. Dependence on ICT vendors and vendor lock-in risks existed in the ICT industry long before organizations started using cloud computing. A large number of ICT products and services are proprietary products, whereby internal data structures and functioning are hidden from the clients and are protected intellectual property. Vendors use this approach to protect their investment in research and development of new products, prevent competitors from copying their solutions and keep the clients tied to their product lines, thus retaining the maximum possible market share. Most often in the ICT world, and especially for software products, when clients purchase a product, they do not obtain its full ownership, but a licence granting them limited rights to use the software under strictly defined conditions.

117. Proprietary technologies are not exclusive to the ICT industry: they are an important aspect of the modern economy and a building element of commercial industries worldwide. However, ICT services are different from other products and services given that clients also make significant investments in technology, developing the expertise for particular technologies and then integrating them, with their data and information (their property), into platforms offered by vendors. The complexity of ICT products and services makes the integration of vendors' products and services and clients' data and resources particularly strong. The effort, complexity and cost of moving from one ICT vendor to another can therefore be very high for large and complex applications.

118. This paradigm from conventional ICT practice extends to commercial cloud computing services. Once an organization starts using cloud-based services, it becomes dependent on particular providers. This dependence arises not only for purely technical reasons, but also as a result of other, general aspects:

(a) Cloud services will quickly contain an important volume of client's data;

(b) The client's staff learns how to use a particular cloud configuration and specific applications from the given provider;

(c) The organization's workflow and business processes are often adapted to a particular software system;

(d) Clients may develop interfaces to link their conventional ICT infrastructure and applications to the particular cloud environment currently hosting their resources.

119. What makes the cloud vendor lock-in different from a conventional ICT service dependence is the fact that vendors continuously update and modify features of their cloud-based services. While this is normally a good practice, there might be situations in which the direction that a service or platform takes does not correspond to the needs and desires of a client. In a traditional, self-hosted, on-premises environment, the client would have the option of simply not upgrading to a new version of the software or not implementing a feature update, at least for a period of time sufficient to consider alternatives or adjust to the changes. With most public cloud-based services, this is not an option, and clients have no control over the changes to the platform features. If the new features are not beneficial for them, they cannot stop them on a public platform that is used by many other users. They would have to either adapt their internal processes to the new features, or consider a migration to a different platform and face the challenges and associated costs of a forced migration.

120. While in theory most providers offer some form of data portability, the actual practical effort necessary to migrate data from one system to a new system offered by a different provider can be considerable, time-consuming and costly.

121. Different services vary significantly in terms of the effort that is required to migrate or replace them. For example, email is one of the easiest services to migrate from one cloud provider to another. Still, migrating archives of old email messages is a considerable workload. Migrating complex applications such as ERP from one cloud provider to another, using different software, is much more complex than migrating email. The complex and interrelated data stored in such applications, in proprietary formats, needs to be exported and converted to the format of the destination system. In addition, the operational and workflow procedures may differ significantly from one system to another, which would require changes in the business processes of the organization.

122. Only one respondent organization (WFP) explicitly mentioned this challenge as being important. In addition, some of the cloud policies and guidelines provided by the respondents included references to exit strategies. For example, the above-mentioned Information Security Special Interest Group white paper contains a section entitled "Barriers to exit", listing issues that organizations should consider in their planning to ensure their ability to switch cloud vendors if necessary. [31]

123. The issue is also identified in the United States Federal Cloud Computing Strategy: "Agencies can consider whether there is a demonstrated capability to move services from one provider to another, and whether there is a demonstrated capability to distribute services between two or more providers in response to service quality and capacity. Agencies should consider the availability of technical standards for cloud interfaces which reduce the risk of vendor lock-in."[32]

124. The issues related to the use of cloud services encountered by United Nations system organizations are also observed in the private sector. For example, the results of a supplier satisfaction survey conducted by EuroCIO, the European association of chief information officers, shows criticism of the major vendors – SAP, Oracle, Microsoft, IBM, Salesforce, Google and Amazon – revealing a substantial and increasing level of dissatisfaction among chief information officers and business users with the vendors' pricing strategies and inflexible licensing and contract management models. The survey revealed a slowdown in cloud adoption and deployment. About 20 per cent of the client base of the main cloud providers were opting to scale down their cloud-based services. Furthermore, recent changes in pricing models generated additional licensing costs and were forcing chief information officers and business users to investigate exit strategies.[33]

125. The cloud infrastructure was not built to provide a public service in a transparent and participatory manner, but, inter alia, to obtain the necessary return on investment required by particular shareholders. The use of cloud solutions is basically the leasing of ICT services provided by privately owned third parties and, as such, there are important risks, outside the direct control of client organizations (for example, company mergers, hostile takeovers and cloud service providers' personnel), that need to be considered and mitigated. While it is true that major providers are reputable, stable and strong firms, it should not be forgotten that they are young companies, privately owned and subject to financial markets laws and upheavals. **While dependence on vendors cannot be ruled out, the Inspectors are of the opinion that organizations should always develop alternative, contingency plans and exit strategies for each critical cloud-based service or application.** Further analysis is perhaps needed to assess the scale of the risk for the system as a whole, which may be different from the risks observed from the perspectives of individual organizations. **The United Nations organizations could also mitigate risks by systematically sharing their experiences of the various cloud service providers.**

D. Interoperability and portability

126. While interoperability and portability are different technical concepts, both refer to the interactions between various components and systems, including those from different vendors, that are necessary for them to work together and the ultimate ability of clients to move or transfer their data and applications between different systems, whether between the cloud services of different providers or between their own system and the cloud services of a provider.

[31] Information Security Special Interest Group, "Use of cloud computing in the United Nations system", p. 18.

[32] Vivek Kundra, "Federal cloud computing strategy", Executive Office of the President of the United States, 8 February 2011, p. 14–15. Available at https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf.

[33] EuroCIO Supplier Satisfaction Survey, the European CIO Association, Press Release, 30 November 2018.

127. Cloud users, whether from business or Governments, have been advocating and demanding standardization of the cloud ecosystem since its early days. However, cloud service providers have only partly responded to this demand and continued developing proprietary solutions that give them a market advantage and make it difficult for their clients to integrate services and products from different providers or migrate from one platform to another.

128. The importance of interoperability in the cloud has been recognized not only by large government agencies that use it, but also by a wider community of users, leading to practical and normative standardization efforts. In 2017, the International Electrotechnical Commission (IEC) and ISO published international standard ISO/IEC 19941, entitled "Information technology: cloud computing – interoperability and portability", in which cloud computing interoperability and portability concepts, types and interactions are defined, with the aim of promoting a common understanding. One of the reasons why interoperability and portability in the cloud is important is that it can help clients mitigate vendor lock-in effects, as discussed above. Another benefit of effective interoperability of cloud services is the ability of clients to integrate their on-premises systems with cloud-based services (even belonging to multiple vendors), creating hybrid solutions that better fit their needs.

129. At the current stage of cloud adoption in the United Nations system, only four organizations explicitly have reported interoperability concerns or challenges. IAEA experienced problems integrating on-premises applications with applications running in the cloud, and the agency had to review and standardize its data to ensure compatibility with the selected cloud service solutions. For WFP, the interoperability concerns were temporary issues related to the initial migration process of mailboxes and archives to the new Office 365 suite, which were easily resolved. FAO reported issues with data portability when using "disparate SaaS solutions". Even though providers offer web services as an option for data interchange, FAO ended up using rudimentary data exchange mechanisms such as file transfer protocol (FTP) and flat files. FAO is working on developing its own middleware solution to facilitate data exchange. A more neutral experience was reported by UNHCR, which encountered cloud-related data portability issues, but found them "not substantially different than problems experienced with any other system migration or integration effort". The Green Climate Fund, which operates exclusively via subscribed and self-made cloud solutions, managed to share data selectively and in real time with partner organizations by developing and providing sets of application programming interfaces.

130. On the positive side, UNICEF reported an increased capacity to handle data transformation and migration, due to the availability of different cloud services, some using the PaaS model, through the cloud platforms that they used.

131. As cloud deployment increases and matures in the United Nations system, the importance of interoperability and portability is likely to grow. This is of particular relevance in the context of increased inter-agency collaboration and the current Secretary-General's reform efforts, including interoperability in the field. While the inter-agency cooperation mechanisms, namely the CEB Digital and Technology Network, are aware of this, **the Inspectors believe that there is a need to deepen collaboration and coordination among United Nations organizations, with the final objective of developing the required compatibility and interoperability of ICT platforms and systems in the field to facilitate joint and/or closely coordinated planning and operations.** While this issue is not a purely technical and depends on complex coordination, a suitable technology could play an enabling role. Cloud computing may be one important tool to achieve this end.

E. Organizational change and cloud adoption

132. The responses to the corporate questionnaire related to acceptance and organizational changes resulting from the use of cloud computing are largely positive and, in some cases, neutral. While a high proportion (50 per cent) of organizations indicated having encountered some challenges related to the migration, they were reported to be manageable and/or resolved. No organizations reported a predominantly negative experience resulting from the use of cloud computing.

133. However, the answers provided by the organizations need to be contextualized, taking into consideration that the extent of the organizational change experienced, as a consequence of the adoption of different cloud solutions, is directly proportional to the magnitude and depth of the cloud solutions being implemented. Obviously, the effect of implementing a cloud-based ERP system is much more significant than that of implementing an SaaS application such as an email system. These examples represent the extremes of a broad range of different possibilities. In practical terms, the implementation of Umoja – the United Nations Secretariat's private cloud ERP system – has had a major organizational impact, yet to be fully assessed, compared to the launch of the new Office 365 email system. According to the United Nations Office at Vienna (UNOV) and United Nations Office on Drugs and Crime (UNODC), "the migration to Umoja … was quite challenging due to the number of business processes covered by the system, including travel, procurement, finance, payment and leave; many operational procedures needed to be changed to match the workflows embodied in Umoja. The migration to Office 365 was simpler and easier, with relatively straightforward acceptance by users."

134. Despite current use of cloud solutions at different levels and for different purposes, most of the respondent organizations have not conducted a comprehensive or deep implementation of cloud services, which is an important element in terms of contextualizing their answers. Furthermore, the Inspectors would like to recall the lessons learned by PAHO, one of the few organizations to have implemented a comprehensive cloud solution. According to the case study on PAHO, the launch of its cloud-based ERP system had profound implications on change management, and "[o]f all the behavioural changes required by PMIS, transformation in the accountability of PAHO managers and the responsibilities of all staff, including managers, along these lines has been, and continues to be, the hardest to achieve."[34] In the view of Inspectors, these are not factors to be neglected.

135. In the same vein, the corporate answers provided by FAO and UNESCO reflect changes observed concerning accountability and responsibility lines between business, including human resources, and ICT units. They reported that these lines needed to be adjusted to reflect the new reality, or, as FAO explained, there was an initial blurring of accountability lines caused by cloud computing. The United Nations Secretariat also indicates an organizational impact of cloud computing, indicating that the process of consolidating disparate governance models to align with the cloud computing services was challenging.

136. The United Nations Secretariat and UN-Women reported that the expectations of end users have risen in terms of the ability to access data from anywhere and using any type of device. Furthermore, UN-Women indicated that "cloud adoption dramatically changes the way we work", and that end users were taking full advantage of the increased accessibility resulting from cloud deployment for advanced collaboration and co-editing. As many cloud applications (of the SaaS type) are designed for direct use by end users and business units, a number of organizations (IAEA, UNOPS and UNRWA) reported that there was a need to adjust operational procedures, which was expected and unproblematic. UNRWA also stated that adjusting operational procedures for the participation of a third party (that is, the cloud service providers) added an extra level of bureaucracy due to the need for additional controls.

137. Further organizational changes reported are more narrowly related to the changes in the procedures and processes of the internal ICT services. UNHCR, UNICEF, UNOPS, WFP and WHO all report adjustment of system- or technical-level procedures resulting from the cloud deployment. While there is little account in the responses provided to the corporate questionnaire of resistance by end users to change, some resistance was encountered by some organizations (UNRWA and WFP) in the context of local ICT administrators losing control and ICT staff facing uncertainty, including future roles and responsibilities. FAO also referred to change management in its response: "[Cloud computing] tends to dramatically impact work structures …. End users can now do more on their own and need less processing assistance from business units that traditionally were involved in the provisioning of that service. These new models bring important changes in the needs of new skills, but also

[34] United Nations System Staff College, "A cloud-based ERP renovates work practices and changes behaviour at PAHO".

'destroy' traditional roles in the organization … which can create strong resistance to the introduction of the new tools." **The Inspectors believe that major decisions to purchase new technological tools should be preceded by wider communications with staff at all operational levels, in particular when new systems might have an impact on staff roles.**

F. Staff skills

138. In order to gain a full view of the organizational impact of the implementation of different cloud computing services, it would also be necessary to assess the impact on staff members and the way in which they undertake their daily work, including new training and other requirements imposed on them by the use of cloud computing. While the views of staff do not directly form part of the present review, the answers provided by the organizations reflecting their corporate views also include elements and aspects of the impact of the use of cloud computing on staff, which have been taken into consideration together with observations and conclusions emanating from the interviews conducted by the Inspectors.

139. Cloud computing is a new technology and, as such, requires specific skills at different levels. However, there are two major groups with significantly different training needs: ICT professionals and the staff at large, or end users. A third group of specialized end users may be considered, which has a need for deeper substantive knowledge in very specific areas, namely users requiring advanced specific, non-ICT-related, knowledge of certain software modules (concerning, for example, accounting).

140. It should be noted that in order to minimize the training needs of end users caused by the constant release of SaaS applications, such applications are often developed with special attention paid to ensuring that their user interfaces are user-friendly and intuitive. In addition, cloud service providers have developed and constantly maintain a wealth of updated training materials for the cloud services that they promote and sell, which are widely available online and are often freely offered to clients. In few cases, organizations have needed to customize these training materials to match their specific needs and products. For example, WHO noted in its response that end users relied on self-help material when using Office 365, which reduced the need for training and support.

141. **While it is true that cloud technologies may facilitate the training of staff, the Inspectors would like to warn against overreliance on the training offered by cloud service providers online. If not properly supplemented by ICT and human resources departments to cater for specific organizational needs, and appropriately managed by managers and staff, such training may not achieve the main expected benefit: a multidimensional, skilled and flexible workforce.** Only one organization (UNWTO) referred to the need to allocate time for staff to undertake the necessary training, indicating that a day of training was offered to all staff members to enable them to familiarize themselves with the new cloud service.

142. In some organizations, staff members are expected to find the necessary time to undertake training. Some provide training targets, such as five days per year, and a list of mandatory training courses to be taken, on very diverse themes ranging from security to, for example, sexual harassment. Cloud-related training is added, online, on top of these requirements, and often cloud services are launched without staff having been properly trained in advance, forcing them to learn by doing. In the view of the Inspectors, this is not often the best approach, particularly when the necessary time is not formally allocated. Some organizations run the risk of neglecting such an important aspect. It is not sufficient or realistic to dump a wealth of knowledge and training materials on online platforms and expect staff to find the right moment to take those specific courses, required for their individual tasks, in time to meet the Organization needs. In the view of Inspectors, a closer look is required at online training systems, including the tools used and the content offered, to maximize the benefits offered by technology. However, that undertaking falls out of the scope of the present review and may be addressed in future by JIU.

143. The new requirements are recognized in the responses provided by some organizations. For example, according to FAO, "the introduction of cloud solutions often forces processes … to take a specific form and as such influence current organizational

structures and ways of working. FAO considers this impact and has considered training in terms of ICT and functional people using the new solutions." Once again, the magnitude of the cloud service being implemented determines the need for staff training. While the opportunistic deployment of a SaaS application may be undertaken with minimal training efforts, other types of implementation will require considerable training, as recognized by UNFPA in its corporate answer: "For some of the future decisions (e.g. ERP system), these needs will be accurately assessed."

144. In addition, the introduction of cloud computing requires ICT units to have new and updated knowledge and skills that are not always available within organizations. FAO noted the need for more specialized skills for managing vendors. This aspect is well recognized in business literature and not a specific problem faced only by United Nations organizations, as confirmed by the Inspectors. For example, the officers interviewed from the World Bank confirmed that it faced the challenge of enhancing in-house skills related, inter alia, to cloud computing. This can be done by hiring staff and consultants to bring new competencies into the organization, but also by providing appropriate technical training. According to UNHCR, "… training … is foreseen for internal staff managing application development and support, and aimed at understanding cloud-native and distributed architectures, as opposed to traditional and vertical application stacks." The United Nations Secretariat in its corporate response referred to the setting up of a cloud centre of excellence, which would include staff who had been trained in cloud technologies, and to an aggressive training schedule that was already provided by Microsoft and Amazon to selected staff for the centre.

145. However, there may be specific situations in which hiring and/or training measures need to be combined with the redeployment of technical resources.

G. Financial challenges

146. The potential costs savings offered by cloud computing have already been discussed in previous paragraphs. However, organizations have also reported some financial and cost-related challenges.

147. The transition from conventional to cloud-based computing requires a change in the structural financing of ICT services. By leveraging shared infrastructure and economies of scale, cloud computing offers a compelling business model. Traditional ICT services require significant upfront capital investments in computing hardware, software, communications infrastructure and the data centre environment in which it is hosted. These are followed by recurrent and relatively evenly distributed operating costs, for maintenance, support, upgrades, migration, disaster recovery, backup and so on. With cloud computing, the initial capital investment is replaced by a pay-per-use model; there is no initial capital investment required and fixed costs are transformed into operating costs. While this is often seen as an advantage of the cloud computing model, it also holds certain disadvantages. In terms of perception, the operating costs triggered by the use of cloud computing – which now incorporate many more elements, including energy, office space and ICT-related staff costs – may appear higher, even if the overall amortized capital costs are much lower than the overall costs incurred in the traditional model.

148. Operational expenditure is always monitored closely and often interpreted as an indicator of an organization's efficiency. An increase in operating costs, resulting from the transition to the cloud or from an increase in usage, due to specific operational needs, that is not related to a significant operational expansion, can be perceived as an inefficient use of resources. In the view of the Inspectors, this is not just a perception issue, but, for some organizations, it represents a structural financial problem, further complicated by the current financial difficulties affecting United Nations organizations and the particular way in which their budgets are prepared and approved.

149. Despite efforts to implement results-based management initiatives in previous years, the reality is that most United Nations organizations have prepared their budgets based on a zero-growth continuity criterion. Operational expenditure is also frequently subject to various restrictions and freezes' even when resources may be available for certain capital investments. Consequently, demands for increases in operational resources have often and systematically

been rejected using a narrow financial criterion, even in cases in which they are well justified from an operational perspective.

150. If materialized, the financial savings emanating from the implementation of a cloud computing solution influence the organization as a whole, although there could be an increase in the specific costs of certain departments and/or units. This is reflected in the corporate response by UNIDO: "Finance departments are not prepared to allow growth of ICT operational expenditures, hampering progress that could otherwise be beneficial on a broader scale. Extrabudgetary resources are typically made available in capital funds, which are not a good fit for investments resulting in cloud services."

151. Consequently, the Inspectors would like to highlight the need to include budget and financial implications, including structural ones, in any risk analysis exercise related to the implementation of cloud computing within organizations. The risk assessment should cover both how to make the transition and how to ensure the sustainability of the service provision. Particular attention should be given to the lock-in effect, which is no different from that of "on-premises systems, and which adds a financial element to the overall implications. There may be cases in which financial strategies need to be updated in order to take account of the changing nature of ICT. Without a change, a number of organizations will not be able to make a transition to cloud computing services, regardless of the extent to which their use cases are justified and their potential gains beneficial.

Recommendation 2

The governing bodies of the United Nations organizations should request the heads of their respective organizations to include provisions in their financial strategies that facilitate the adaptation, responsiveness and efficient use of operational expenditures and capital investments related to new technologies.

152. The World Bank refers to a lack of economies of scale when using cloud computing. There are economies of scale that result from owning an entire data centre. Adding one more server is cheaper than the acquisition of the first. In the cloud, every central processing unit and gigabyte needed will cost the same, but the client pays for those additional computing resources only when used. This can also make it more challenging to predict monthly costs, since a sudden increase in usage of an application can result in a sudden jump in actual costs.[35] The United Nations Conference on Trade and Development (UNCTAD) noted in one report, that the potential risks of increased costs for communication and for migration and integration, as well as other challenges already described above, are worthy of consideration in relation to cloud computing.[36]

153. Most organizations embark on a transition to cloud computing expecting to achieve cost savings, among other reasons: 11 organizations listed direct cost savings as part of their motivation for using cloud computing. Four organizations reported that it was too early for them to assess whether expected savings have materialized, while seven organizations had completed a formal analysis of cost and efficiency benefits. In total, nine organizations reported observed gains, including some that did not complete a full analysis.

154. However, cloud deployment may in some cases result in unexpected costs because of incomplete or deficient analysis, delayed adaptation to the cloud model, or as lack of transparency or subsequent changes in the cloud service provider's policy or services. The reports of unexpected costs that were reviewed do not reflect a large-scale issue, though, and some are of a temporary nature, related to the migration of legacy systems. Being aware of such unexpected costs may be useful for organizations that are yet to embark on cloud computing or are in the early stages of their projects, and help them to better plan and avoid mistakes.

[35] World Bank, "Cloud computing overview", pp. 16–17.

[36] *Information Economy Report 2013: The Cloud Economy and Developing Countries* (United Nations publication, Sales No. E.13.II.D.6), p. 5.

155. UNWTO reported an unforeseen cost of data storage capacity, while it achieved printing cost reductions and time savings resulting from the distribution of documents via their cloud-based file-sharing system. UNDP referred to an "[e]scalation of post-contractual costs due to application of 'in-house data centre' paradigms like overprovisioning capacity and challenges to properly estimate future usage". It also reported additional unforeseen costs due to the need to upgrade certain software licences that were required to improve security protection.

156. In its corporate response, ICAO referred to some unforeseen costs related to training, information security and segregation of environments, resulting from the implementation of industry best practices, which required more cloud resources than initially anticipated. At the same time, ICAO reported improvements in its service capacity as part of its analysis of efficiency gains.

157. FAO referred to cost savings and important improvements in compliance and user satisfaction, also noting unforeseen costs related to organizational change management. It reported an ongoing revision of the network model and infrastructure, which was needed to support better connectivity to the cloud. It should be noted that connectivity might be an issue given the required network bandwidth of cloud adoption on specific categories of applications (such as systems that are currently deployed locally on users' personal computers). In these specific cases, moving the applications to the cloud often requires an increase in the quality and quantity of connectivity services available in a specific geographical location. Not only is this element a cost factor that may increase, but it also poses specific risks of unavailability of the functions necessary for the provision of services.

158. Similarly, the Green Climate Fund reported significant cost savings overall, but registered additional costs for integration, maintenance and end user support when compared with an on-premises or private cloud scenario. WHO reported additional costs and complexity related to a proprietary layer of data encryption, which was being removed following an initial trial period.

159. **The Inspectors therefore recommend that the estimated financial benefits be rigorously and thoroughly analysed by organizations before contracting cloud computing services.**

H. Data privacy and confidentiality, including the United Nations privileges and immunities

160. Cloud computing enables global availability of information; however, its intrinsic nature, characterized by remote access and distributed processing, poses risks concerning data and information privacy. Protecting data and information is imperative to Governments, organizations and enterprises worldwide. There are two different perspectives on data privacy and confidentiality: legal and technical. While the technical perspective may be concerned with security – discussed in the section on new security requirements above (chap. III, sect. B) – the misuse of confidential data is a risk of a legal nature to be addressed, inter alia, in the wider context of the protection of privileges and immunities of the United Nations, the specialized agencies and IAEA, as defined in the Convention on the Privileges and Immunities of the United Nations (1946) (see box 6 below), the Convention on the Privileges and Immunities of the Specialized Agencies (1947) and the Agreement on the Privileges and Immunities of the International Atomic Energy Agency (1959).[37]

161. The legal and technical dimensions of data security and confidentiality have been identified by respondent organizations as a major challenge in their implementation of cloud-based solutions. Twelve organizations reported challenges related to United Nations privileges and immunities, while nine organizations explicitly reported data security and confidentiality among the major challenges.

[37] United Nations, *Treaty Series*, vol. 374, No. 5334.

162. With the use of cloud computing, data and information, travelling over the Internet or broadband networks, may be stored and replicated for backup purposes in any, or several, of the geographical areas in which cloud service providers operate. This may pose legal concerns with respect to the extraterritorial nature of data and the applicability of the national legal frameworks of those countries in which the data are hosted.

Box 6

Convention on the Privileges and Immunities of the United Nations

Article II:

PROPERTY, FUNDS AND ASSETS

Section 2. The United Nations, its property and assets wherever located and by whomsoever held, shall enjoy immunity from every form of legal process

Section 3. The premises of the United Nations shall be inviolable. The property and assets of the United Nations, wherever located and by whomsoever held, shall be immune from search, requisition, confiscation, expropriation and any other form of interference, whether by executive, administrative, judicial or legislative action.

Section 4. The archives of the United Nations, and in general all documents belonging to it or held by it, shall be inviolable wherever located.

163. Numerous countries have developed specific laws and frameworks to address gaps in the legal coverage of data protection.[38] These regulations intend, inter alia, to tackle the impact of new technologies and manage cross-border data transfers, including determination of the jurisdiction to be applied in different cases. These regulations are also aimed at addressing the need to balance government reach for security purposes against the privacy rights of the individuals owning the data. Major initiatives launched worldwide include the following:

(a) The European Union issued its new General Data Protection Regulation, or GDPR (regulation (EU) 2016/679 of the European Parliament and of the Council of the European Union of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)), to replace the European directive on data protection (directive 95/46/EC of the European Parliament and of the Council of the European Union of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data), which had been a prominent source of regulation for 20 years. GDPR became fully enforceable throughout the European Union in May 2018;

(b) Data privacy protection has been included in several international trade agreements;[39]

(c) The United States Clarifying Lawful Overseas Use of Data (CLOUD) Act was enacted in 2018;

(d) The European Union and the United States renegotiated a cross- border data protection agreement (the former EU-US Safe Harbour Framework, now known as the EU-US Privacy Shield).

164. The Inspectors noted some confusion among several officers interviewed with respect to the applicability of the above regulations to United Nations organizations, which was partly caused by the timely coincidence of the recent introduction of GDPR and the CLOUD Act with the preparation of the present review. Since chapter V of GDPR refers to data transfers to international organizations, it appears that the GDPR might affect flows of personal data to international organizations. In turn, under the CLOUD Act, United States

[38] A total of 107 countries have data privacy laws, and several countries are revising their laws. See the UNCTAD Global Cyberlaw Tracker, available at https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Global-Legislation.aspx.

[39] Article XIV (c) (ii) of the WTO General Agreement on Trade in Services permits measures necessary for “the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records”.

law enforcement may serve warrants or subpoenas on server-stored data, regardless of the physical location of the servers, as long as the service provider is based in the United States. The Act also allows for "executive agreements" that would give foreign Governments the right to access data in the United States without regard for United States privacy laws, without informing those involved and without judicial review. The law is supported by technology companies and service providers and opposed by advocates for privacy and human rights.[40]

165. A fundamental distinction between GDPR and the CLOUD Act is that GDPR requires prior consent by the data owner to share his or her data, while the CLOUD Act does not include any requirement to provide consent by the data owner prior to the execution of the warrant. In this sense, GPDR is seen as advancing data privacy rights. In order to face subpoenas and protect from requests for information and data from third parties, including Governments, some organizations are forced to include legal clauses in their respective cloud computing contracts requesting providers to inform them before sharing any of their data and information. For example, the United Nations Secretariat indicated that "… the vendor will make a good faith effort to flag United Nations-related third-party requests for data and advise the third-party requestor that such data belongs to the United Nations and subject to certain privileges and immunities … the open nature of the public cloud means that United Nations data could be seized pursuant to subpoenas .... Consequently, use of public cloud services entails acceptance of certain limits on data privacy and less control over preventing third-party access to United Nations information. The Organization cannot, therefore, eliminate the risk that a third party will gain access to United Nations data in its use of such online services." The United Nations Secretariat concludes that "… highly sensitive data should remain internally managed. Accordingly, OLA [the Office of Legal Affairs] had advised that should the Secretariat consider enrolling in the Online Services in the future, it is advisable that the levels and sensitivity of different data be determined and categorized."

166. In addition to the above initiatives, the Inspectors welcome the establishment by the United Nations Global Pulse initiative[41] of a data privacy advisory group, comprising experts from the public and private sector, academia and civil society, as a forum to engage in a continuous dialogue on topics related to data protection and privacy. They also welcome the development of the Personal Data Protection and Privacy Principles for the United Nations system organizations, which were adopted by the High-level Committee on Management at its thirty-sixth session, on 11 October 2018.

167. The Principles set out a common framework intended to protect the right to privacy, with the following aims: (a) harmonize standards for the protection of personal data across the United Nations system organizations; (b) facilitate the accountable processing of personal data for the purposes of implementing the mandates of the United Nations system organizations; and (c) ensure respect for the human rights and fundamental freedoms of individuals, in particular the right to privacy.

168. **In the view of Inspectors, digitalized data are a form of assets, which are referred to in the provisions of the Convention on the Privileges and Immunities of the United Nations and the Convention on the Privileges and Immunities of the Specialized Agencies. Thus, any information owned by United Nations entities and stored by third-party cloud service providers, regardless of the storage location, should be subject to these immunities. Given their international and higher-level nature, the United Nations immunities may override the prevailing applicable national and regional regulations, particular taking into consideration that such regulations may emanate from countries which are Member States of the United Nations and have ratified those Conventions or benefit from them.**

169. Nevertheless, in an effort to clarify the matter, the United Nations Legal Network requested guidance and clarification on the legal framework to be applied to United Nations

[40] See https://nsarchive.gwu.edu/news/cybervault/2018-04-02/hr-4943-clarifying-lawful-overseas-use-data-act-cloud-act.

[41] Global Pulse is an initiative of the Secretary-General on big data, and a vision of a future in which big data is harnessed safely and responsibly as a public good. Its mission is to accelerate discovery, development and scaled adoption of big data innovation for sustainable development and humanitarian action. See www.unglobalpulse.org/about-new.

organizations, including questions regarding the non-applicability of GDPR. The answer provided by the European Union confirmed that GDPR was not applicable to United Nations organizations. However, given its recent enforcement and the very different usages of data made by organizations, ranging from sensitive refugees' personal data to suppliers and/or staff-related data, **the Inspectors recommend organizations to further analyse the implications of GDPR and other similar regulations in light of their own operational activities, including the necessary requirements to be met by their implementing partners, which might not be subject to the same privileges and immunities.**

170. The Inspectors confirm that organizations are well aware of the data confidentiality risks that depend on the geographical locations used by their third-party vendors. Organizations often benefit from the fact that most cloud vendors allow clients to choose the specific data centres in which processing, storage and backup will take place, and therefore the geographical location of their data. For example, ILO indicated that contractual terms stipulated where servers and data could be located. However, not all cloud service providers offer this possibility, as confirmed by UNFPA in its corporate answer: it stated that the service provider (Google) had a number of data centres and UNFPA data was likely stored in all of them, and it did not have control over the location of the servers. UNWTO added that one of the reasons why it had not moved forward to cloud services was that there was no guarantee that such services could cover United Nations privileges and immunities; its current service, ShareFile, used servers located in Europe only. Other United Nations organizations and specialized agencies request the cloud service provider to keep their data in locations in which privileges and immunities are respected. For example, UNDP requested that the tenancy of Office 365 be associated with the data centre in Ireland to ensure that its data fell under the jurisdiction of the European Union privacy laws.

171. **The Inspectors reiterate and stress the need to include in relevant contracts the specific geographical locations of the servers to be used for the processing and storage of United Nations data and information, taking into consideration the respect and protection of privileges and immunities offered by national authorities in those locations.**

I. Data classification and the need to enforce policies

172. Most of the United Nations organizations have developed data classification policies, and only two organizations (UNWTO and WMO) revealed that relevant policies were under development or not in place. Data classification policies establish the criteria for different levels of data sensitivity and, though the specific terminology used by organizations may differ, the levels range from strictly confidential to data that can be made openly available to the public at large. Policies also refer to the specific procedures to be applied to the different levels of confidentiality. It should be noted that a number of organizations have not updated their data and information classification policies to take into consideration the new challenges posed by new technologies such as cloud computing.

173. Some organizations have information security awareness campaigns in place. However, despite the availability of policies and technical tools required to safeguard data confidentiality, **the Inspectors observed a lack of enforcement of the relevant policies, as confirmed by several officers interviewed, who referred to blurred lines of responsibility between ICT units, responsible for the technical implementation, and substantive units, responsible for the appropriate classification when data and information are created.** In the view of the Inspectors, additional efforts must be made to implement and comply with data classification policies.

174. While several officers interviewed believed that all types of data, including restricted confidential data, could be stored in cloud-based systems after the establishment of appropriate security measures, several organizations had concluded that highly sensitive data should not be stored in third-party cloud-based systems. UNESCO, for example, indicated that it had not identified any specific data that could not be shared in the cloud, but that if the data were classified as strictly confidential, the cloud should never be used.

175. **The Inspectors recommend that organizations that have not yet done so develop or update data classification policies to take into consideration the Personal Data Protection and Privacy Principles and the challenges posed by the use of cloud-based systems.** Data classification policies should make reference to relevant monitoring and enforcement mechanisms.

J. Some conclusions

176. There is significant variety between the United Nations organizations in their approaches to cloud computing services and in their degrees of adoption of cloud computing. There are (a) a few organizations that do not use cloud computing services, (b) organizations that fully depend on the cloud, and (c) many organizations in between that use the cloud to some extent. Still, some general and technical trends can be identified as common to a number of organizations, as follows:

(a) Most organizations are moving some of their computing capacity to the cloud;

(b) Cloud computing is used in different forms: cloud-based ERP solutions, the provision of cloud services by United Nations organizations as the cloud service provider, as the client of various cloud services and so on. However, the biggest push towards the cloud seems to be in adopting email and productivity applications provided as cloud services, mostly based on Microsoft Office 365;

(c) Most organizations have chosen one of the handful of biggest public cloud providers for productivity and mainstream business applications. Reputation is a key factor in selecting a provider;

(d) Cost reduction, simplification, flexibility, agility, better perceived security and innovation are among the most cited reasons for moving to the cloud;

(e) There is no one dominant cloud computing approach or trend among the organizations: there is significant diversity in the deployment approaches and stages in the United Nations system;

(f) Services models are chosen according to the functionality and benefits desired, and in some cases according to the availability of services of a particular form.

177. Some organizations have a clear inventory of all potential or expected benefits of cloud computing and have developed mechanisms to facilitate the implementation and monitoring of cloud-based services, clearly mapped into the organizations' respective ICT strategies. **The Inspectors believe that in the absence of a self-standing cloud computing strategy, priorities and initiatives must be identified and added to the organizations' respective ICT strategies regularly in order to facilitate monitoring and accountability.**

Recommendation 3

The executive heads of the United Nations organizations should put in place periodic procedures to ensure that their corporate ICT strategies, including those for cloud computing services, are aligned with the organizations' business needs and priorities, and yield value for the investment.

178. However, in order to for the potential benefits offered by cloud computing to be realized, organizational ICT requirements need to be determined first, taking into consideration, inter alia, current ICT infrastructure, legacy systems and applications that were not originally designed for the cloud and may have to be updated, a time-consuming undertaking. It should be noted that not all organizations should move to the cloud. Using an SaaS application is not the same as implementing an IaaS solution. Before selecting a service or deployment model, organizations first need to consider the benefits and risks of moving to the cloud.

179. United Nations organizations began their cloud migration with low complexity services in order to build capacity and progressively mature their approach to more complex

ones. Annex II shows that most of the United Nation organizations use low complexity services such as Microsoft Azure Storage and Microsoft Office 365: these services often do not include the use of sensitive data, making the migration to cloud services more straightforward.

180. However, even those organizations that started their journey to the cloud with relatively easy or less complex applications find themselves second-guessing their original assumptions. For example, during the interviews held by the Inspectors, including joint meetings with technical management, legal and procurement representatives, it was frequently stated that organizations had decided to use cloud services with the expectation of reducing costs and realizing the promise of cloud benefits. Some of the potential benefits of the cloud have a downside, however, in areas such as security and cost, which are also perceived as challenges by some organizations. There is a lack of clarity on where and how the savings will materialize and a lack of confidence in the safe storage of highly sensitive data in the cloud, and there are some cases of increases in short-term costs. Organizations often find themselves without the skills needed to harness the opportunities presented by the cloud.

181. In conclusion, cloud computing offers an opportunity for higher efficiency, new functionality and lower costs, However, the opportunity needs to be realized through comprehensive planning and consideration of the multiple dimensions affected by the use of cloud services, namely technical, financial, legal and managerial. Furthermore, cloud computing comes with significant risks that need to be mitigated through contextual risk assessments.

Recommendation 4

The executive heads of the United Nations organizations should ensure that a comprehensive risk analysis exercise is undertaken before contracting ICT services, including cloud-based services. The risk analysis exercise should consider both technical and financial risks and benefits, and relevant safeguards should be included in the service-level agreement.

182. Overall, the United Nations system follows the wider trend of commodification of computing services and cloud adoption. The primary driving forces and considerations for using cloud services are most often similar to those of enterprises worldwide. Specific conditions related to the nature of United Nations organizations rarely have an impact on the decision to use cloud computing. According to the Information Security Special Interest Group, cloud computing allows United Nations agencies to establish what is essentially a virtual facility and achieve the flexibility of connecting to business applications and information from anywhere and at any time.

183. Organizations undertake ICT investments with the expectation of greater efficiency and effectiveness in the functioning of the organizations. **The Inspectors would like to emphasize that ICT projects including cloud computing represent strategic investments for organizations, which require close monitoring and reporting mechanisms.**

184. **In conclusion, when migration to the cloud is envisaged, organizations should take into consideration several factors that address the issue in all its complexity, including the following:**

(a) Revision and enforcement of data classification policies, taking into consideration the new Personal Data Protection and Privacy Principles and the challenges posed by the use of cloud-based systems, including the implications of GDPR and other similar regulations;

(b) Exploration of potential to improve collaboration and coordination between United Nations organizations by developing a joint approach or framework for the use of cloud computing services, including a set of common basic requirements to be implemented across the system;

(c) Identification in the relevant contracts of the specific geographical locations of the servers on which United Nations data and information are stored and processed, and measures to ensure respect for and protection of privileges and immunities in those locations;

(d) Comprehensive risk assessments as a key mandatory step in any consideration of cloud computing solutions;

(e) Development of contingency plans and exit strategies for each critical service or application based on cloud computing;

(f) Mitigation of risks by including pertinent safeguards in SLAs.

IV. Decision-making practices and the use of service-level agreements

185. It can be concluded that the use of cloud computing is more than a technological challenge. It may also have a significant impact on organizational change management, affecting different aspects of the governance, security, efficiency and financing of organizations, as described above. **Consequently, there is an evident need within organizations for comprehensive decision-making practices that include the different organizational units and go beyond technical considerations when contemplating any form of technology adoption, including cloud-based services.** Furthermore, given the challenges posed by cloud services and the appearance of third-party actors, the selection and use of cloud-based services requires the establishment of appropriate due diligence processes and the preparation of comprehensive SLAs,[42] which must be seen not only as a legal protection mechanism but also as a tool to effectively manage relations with cloud service providers on the basis of objective output metrics.

186. A number of responses provided by organizations indicate that the strong initiative of internal ICT units plays a major role in the adoption of cloud-based systems, although initiative can also emanate from substantive units in need of a specific solution. Most decision-making processes established by organizations require a risk analysis to be undertaken, followed by technical and managerial clearances by relevant committees. Several questionnaire responses indicated a broad consultation process within organizations as part of the decision-making process, regardless of whether the source of the initiative was ICT units, business units or general management. Such consultations are mostly carried out in the context of adopting cloud-first or comprehensive cloud strategies. This pattern suggests that cloud adoption has been thoroughly analysed and considered from various angles (technical, legal, financial and human resources). This point was confirmed by the Inspectors through their interviews with managers, procurement and legal officers, who generally confirmed their involvement in their respective organizations' consideration of cloud-based services.

187. In the view of the Inspectors, the procedure established by the United Nations Secretariat, entitled "Cloud computing: United Nations Secretariat ICT technical procedure" and issued in 2017, can be considered an example of best practice, which is intended to describe the requirements for the acquisition and use by the Secretariat of cloud computing services provided by external cloud service providers. It also specifies requirements to ensure that such services meet the United Nations business, operational and security requirements, mitigating risks that may affect the business continuity and security of ICT resources. Appendix 1 of the Secretariat's technical procedure, entitled "Evaluating cloud service providers and cloud SLAs" (see box 7), contains the necessary elements to be taken into consideration when preparing SLAs for cloud-based services. These normally include, inter alia, performance levels and targets, security controls and limitations, data storage locations, business continuity, and legal and service requirements and safeguards.

188. However, measuring and validating the status of compliance of cloud vendors against various criteria, including those in relevant SLAs, can be challenging, because cloud service providers often rely on subcontractors to provide services. Furthermore, although SLAs include penalties in case of infringement of the established conditions, such penalties are not considered an important negotiating factor by some organizations. For example, the United Nations Secretariat indicates that "the Office of Legal Affairs (OLA) advises against including 'penalties' in procurement contracts as such provisions are generally found unenforceable on grounds of public policy". IAEA also confirms this point: "SLAs with the largest, most attractive suppliers are generally not comprehensive or negotiable, and rarely provide for adequate penalties to remediate a loss. Despite this, it is still imperative to

[42] A cloud SLA includes terms that provide details of the level of service provided by a cloud service provider in order to meet the business requirements of its consumer. The cloud SLA typically comprises service promises, limitations and consumer obligations. "Cloud computing: United Nations Secretariat ICT technical procedure", appendix 1 "Evaluating cloud service providers and cloud SLAs: overview", March 2017.

leverage these providers because their reputation matters more than the penalties." **The Inspectors recommend a rigorous analysis of all requirements to be included in SLAs, as described in appendix 1 of the Secretariat's technical procedure.**

189. **The Inspectors also firmly believe that United Nations organizations should actively monitor SLAs and hold vendors accountable for any failure to comply with the requirements established. In the Inspectors' view, information on cloud service providers' performance should be systematically shared at the system-wide level.**

190. The most significant example of SLA used by several United Nations organizations is for Microsoft Office 365. Originally negotiated by UNDP, the agreement is also used by other United Nations organizations (including the Secretariat, UNESCO, UNICEF and WHO). The Inspectors welcome this joint approach and stress the advantage of joint negotiations in an effort to leverage the purchasing power of the United Nations system. A joint approach may bring cost benefits but, more importantly, it also brings standardization, efficiency and interoperability benefits, which are difficult to quantify. Other entities with complex administrative structures have identified the need to aggregate demand, such as the United States Government: "When considering 'commodity' and common [ICT] services, agencies should pool their purchasing power by aggregating demand to the greatest extent possible before migrating services to the cloud".[43]

191. The WFP ICT framework for cloud computing serves as another example of the involvement of different organizational units when contemplating cloud-based solutions. It includes the WFP cloud computing position paper, a document on WFP corporate information and ICT security, a WFP corporate information technology strategy for the period 2016–2020, and a document on technical approval for the procurement of ICT software, hardware and services.

192. The WFP cloud computing position paper is the framework's core. It covers the characteristics and service models of cloud computing, aligns WFP

Box 7

Evaluating cloud service providers and cloud SLAs

A cloud SLA includes terms that provide details on the level of service provided by a cloud service provider in order to meet the business requirements of its consumer. The cloud SLA typically comprises service promises, limitations and consumer obligations.

Service promises and commitments usually include:

(a) Performance: availability and accessibility, capacity, interoperability and open interface, and support levels;

(b) Retention and storage location(s);

(c) Remediation process in case of SLA violation (e.g. service credits);

(d) Security controls and data protection;

(e) Legal requirements and protection of consumer information and personal data.

Service limitations usually include:

(a) Scheduled service outages: these might be excluded from the availability requirement;

(b) Force majeure events;

(c) Service changes and notification process;

(d) Security limitations;

(e) Legal obligations;

(f) Service application programming interface changes.

Consumer obligations usually include:

(a) Provider acceptable use policies;

(b) Conformance to software licence terms;

(c) Timely payment.

Source: United Nations, "Cloud computing: United Nations Secretariat ICT technical procedure, appendix 1, March 2017.

[43] Kundra, "Federal cloud computing strategy", p. 15.

with the white paper issued by the Information Security Special Interest Group in terms of risk mitigation, sets standards for WFP sourcing of cloud services and establishes the roles and responsibilities of cloud computing management.

193. With regard to roles and responsibilities, the paper provides for a cooperative inter-unit approach when deploying cloud computing services. The process includes a comprehensive risk assessment, whereby business units and data owners determine the relevant levels of data sensitivity and the ICT division conducts the ICT security and other technical evaluations in order to identify concerns and ensure appropriate protections.

194. The WFP Legal Office, in coordination with the ICT division, specifies the legal terms and conditions under which WFP ICT services and/or data can be hosted or managed in a hybrid or public cloud, and ensures that the legal interests, rights, privileges and immunities of WFP are contractually protected by appropriate legal safeguards before signing a contract with public cloud service providers. In so doing, the Legal Office supports both the requesting unit and the ICT division during the procurement planning and negotiation phases of cloud service contracts to ensure that the terms offered by the providers meet the compliance needs of WFP.

195. A comprehensive SLA that clearly sets out the responsibilities and accountability of cloud service providers is key for the acquisition and appropriate use of external providers' cloud computing services. Since joint procurement might not currently be possible, all United Nations organizations should collaborate to leverage better terms and conditions. The Inspectors identified good examples of inter-agency collaboration, but could not find detailed provisions in procurement regulations to facilitate collaboration among organizations when purchasing cloud services. **In the Inspectors view, in order to increase procurement collaboration in the system, United Nations system organizations should include specific provisions on collaboration in their procurement regulations, including general terms and conditions of contracts for cloud computing.** The Procurement Network of the High-level Committee on Management should play a greater role in harmonizing and fostering collaborative procurement.

V. United Nations system cooperation and the United Nations International Computing Centre

196. The primary mechanism for United Nations system-wide cooperation in the context of information technologies is the Digital and Technology Network, formerly the ICT Network, established under the umbrella of the High-level Committee on Management. It provides, inter alia, a forum for the discussion of new opportunities for inter-agency collaboration and the sharing of relevant practices regarding the use of ICT by United Nations organizations.

197. The ICT Network, at its thirty-first session, in October 2018, decided unanimously to rename itself to the Digital and Technology Network in recognition of the need to extend the Network's focus towards a strategic and digital transformation of the United Nations system as a whole. It is a shift in focus from the operational and tactical towards a strategic collaboration in programmatic and frontier activities.[44]

198. The Digital and Technology Network presently oversees the activities of the Information Security Special Interest Group and the ERP Special Interest Group. The Information Security Special Interest Group is the main mechanism within the United Nations system for the promotion of inter-agency cooperation and collaboration on matters related to information security. Its primary objective is the optimization of information security within its member organizations. An additional three special interest groups were established by the Digital and Technology Network at its thirty-first session, on technology innovation, infrastructure transformation and business transformation.

199. The Inspectors welcome these initiatives, which are relevant and timely in the context of the present review. In particular, they welcome the establishment of the Infrastructure Transformation Special Interest Group: sponsored by IAEA, this group is responsible for considering the migration of organizations' infrastructure to the cloud and related trends in order to share knowledge and experiences.

200. However, on the basis of their analysis of responses to the corporate questionnaire, **the Inspectors believe that system-wide cooperation should go beyond sharing knowledge and experiences**. Seven organizations, about a third of respondents, indicated that they did not use cloud computing services in association with other United Nations organizations, and some call for increased cooperation. UNESCO indicated that it had been clear from the last ICT Network meeting that the vast majority of United Nations organizations were using or starting to use Office 365, and "we have agreed to federate Skype for Business … there is quite some opportunity to work together in this area. All the mentioned applications are used by multiple other United Nations agencies. We have had contact with them to share experiences, and this has been input to our decision processes." UNICEF also referred to the benefits of actual cooperation: "We have already experienced some advantages in terms of integration and collaboration with other agencies that also use Office 365 and Azure Active Directory."

201. One of the main potential advantages of cloud computing is scalability. From that perspective, there are benefits that come only from economies of scale at the system-wide level. Furthermore, certain challenges can be better confronted by acting together. For example, all organizations should stay ahead of emerging security threats and ensure that their security outlook is constantly evolving. They also need to ensure that they retain an appropriate level of control to effect changes in security that are in their best interest. The pooling of resources could optimize the use of expensive resources at the system-wide level while making a range of higher-quality services accessible to smaller organizations. Such considerations fuelled the General Assembly's vision that underpinned the establishment of UNICC.

[44] Chief Executives Board for Coordination, "31st Session of the ICT Network, New York, 23–24 October 2018: meeting summary", document CEB/2018/HLCM/ICT/18, executive summary.

A. United Nations International Computing Centre: a system-wide service provider

202. UNICC was created by the General Assembly in its resolution 2741 (XXV) in 1970 to provide electronic data processing solutions for the United Nations system. Its mission includes:

(a) Providing a technology and procurement hub and associated ICT services to the United Nations family and related international organizations;

(b) Maximizing the sharing of infrastructure, systems, solutions and expertise;

(c) Generating economies of scale to benefit clients.

203. UNICC has over 50 clients and partner organizations and more than 400 staff and contractors. It has offices in Switzerland, Spain, Italy and the United States and data centres with United Nations jurisdiction for the safeguard of privileges and immunities. It offers a wide range of services, including support for private, hybrid and public cloud solutions. UNICC is a provider of ICT managed services, and has the capacity and technical expertise to support the various cloud service models (IaaS, PaaS and SaaS). UNICC is committed to delivering quality ICT services, maintaining its ISO/IEC 20000-1 and ISO/IEC 27001 certification for all services, maintaining appropriate levels of information security controls and undergoing independent audits based on international standards.

204. UNICC currently provides a range of services to the majority of United Nations organizations. The following is non-exhaustive sample of its various services and clients. UNICC hosts several ERP systems (FAO, IAEA, UNDP, UNHCR, WFP and WHO), and provides disaster recovery and business continuity services (ILO, International Maritime Organization (IMO) and UNESCO), as well as professional services to others (UNHCR, UNICEF, UNIDO, UN-Women, WFP and WMO). In this context, UNDP and UNICC have engaged in a partnership whereby, in 2017 and 2018, UNICC evaluated cloud market solutions for UNDP and, in 2019, UNDP tasked UNICC with performing the technical upgrade of its ERP system, Atlas.

205. While the answers provided by the organizations confirm significant use of UNICC products and services, they also point to a number of issues preventing further growth. Several officers interviewed referred to the lack of competitive prices, or to the lack of advanced technical support when compared to major cloud service providers. In the view of Inspectors, this comparison is not realistic, or necessary. UNICC was not created to compete with private sector cloud service providers, which have a wealth of resources that is unavailable in the United Nations system. In addition, the private providers are primarily motivated by generating profit, emphasizing measurable parameters and perceived immediate benefits, such as cost-efficiency or innovation, even at the expense of the longer-term needs of their clients.

206. Cost considerations are a determining factor for organizations when purchasing services and products. In order to guarantee the cost-effectiveness of the services provided by UNICC, the General Assembly, in its resolution 63/269 of 7 April 2009, requested the Secretary-General to ensure compliance with all regulations and rules regarding procurement when utilizing the services of the UNICC. Some organizations reflected cost concerns in their corporate answers (UNEP, UNESCO, UNWTO and WHO) and others criticized the administrative and invoicing complexity of UNICC procedures, although some of them also found the billing of some public cloud services even more complex.

207. Nonetheless, there seems to be a discrepancy between the critical perceptions of UNICC among some of its clients and the growing use of its services and products. While UNICC indicates that it provides a wide variety of standard and custom cloud computing services to meet client requirements in different cloud environments, the United Nations Secretariat in its corporate answer indicated: “The Department of Management/OICT does not use the services of UNICC but the Department of Field Support uses UNICC for operations support. UNICC, as far as OICT is aware, does not have cloud computing services

in its portfolio."[45] This perception is evident proof of the need to enhance communications at the system-wide level. In its comments on the final draft of the report, dated 15 May 2019, the Secretariat specified: "OICT is fully aware of all service offerings from UNICC ... However, at the time when the questionnaire sent by JIU was finalized, UNICC did not have any cloud-based services. In fact, only at the last [meeting of the] UNICC Management Committee, of 26 March 2019, members of the Committee endorsed the establishment of the cloud computing service."

208. A value-for-money benchmarking study was conducted in 2017 by Maturity GmbH at the request of the UNICC Management Committee, covering UNICC operational activities for its top seven services by income. The key findings showed that, overall, UNICC prices were lower than those of the peer group, and could be even lower if the services were further standardized; that customer awareness of service levels, complexity and value was low due to a lack of effective communication from UNICC; and that customer satisfaction had been positive.

209. Another factor to consider is that UNICC does not have regular funds for research and development. Considering the pace at which cloud platforms and related services are currently evolving, it is somewhat difficult for UNICC to keep pace with commercial providers, especially when it comes to user-facing features. While the fundamental data-centre infrastructure and services are excellent and very much up to date, the user-facing features can seem outdated or inferior if not constantly updated and improved.

210. **The best value for money should be the prevailing decision-making factor when considering cloud services. However, the Inspectors are convinced that, notwithstanding such considerations and the competitiveness of UNICC with other cloud service providers in this area, it is unnecessary and simply unrealistic to compete with the major providers. United Nations organizations and UNICC should find areas in which shared services could be provided at a reasonable cost using the UNICC hub to leverage its expertise, including research and development capacity, and complementing their own, without requiring additional and costly expertise in-house within each organization.**

211. UNICC is traditionally more experienced with managed services, in line with clients' perceptions, than with cloud solutions. It is characterized by a customer-service culture and the readiness to customize services to a high degree, according to the context and needs of the client. While this provides a strong value added element for customers, it does not help with cost reduction. In addition, maintaining outdated platforms for clients makes it difficult to maintain the ISO and security standards of the infrastructure used and deployed. Due to its mandate, and in contrast to commercial cloud service providers, UNICC safeguards clients' interest by, inter alia, reducing their costs (such as by monitoring and reporting unused resources, such as mailboxes).

B. Governance of the United Nations International Computing Centre

212. The management structure of UNICC comprises the Management Committee, composed of one representative from each partner organization, and a secretariat. Partner organizations provide information to support the annual business planning process of UNICC. The business plan should extend beyond the financial cycle of a single year or biennium. The information provided must include, inter alia, indications of new work intended for UNICC, either through the adoption of services already available but not yet used by the partner organization or through the identification of a need for a service that UNICC does not yet provide.

213. The Inspectors note that most of the United Nations organizations are represented in the Management Committee. The organizations therefore have a mechanism to drive UNICC, including its cloud strategy, to better fit and supplement their business needs, including on

[45] For a detailed description of cloud services offered by UNICC, please see UNICC, "ICT Services", April 2018. Available at www.unicc.org/wp-content/uploads/2018/08/ICC-ICT-Services.pdf.

research and development. However, that mechanism should be empowered and delegated with enough authority to contribute to system-wide synergies.

214. The UNICC particular structure and governance model, while providing opportunities, also results in some challenges that need to be resolved to enable further strengthening and growth. The representatives of partner organizations on the Management Committee happen to be mostly technical representatives, either chief information officers or chiefs of ICT units. On the one hand, this is useful as it allows the Committee to understand the technical aspects of the strategy and operations of UNICC. However, when priorities diverge, it may be inevitable that representatives give priority to the particular interests of the organizations that they represent over the broader interests of the United Nations system as a whole or those specific to UNICC. In the view of Inspectors, this may pose a perceived conflict of interest, given the coincidence of roles: first as decision makers in their capacity as members of the Management Committee, and second as directly affected parties or primary beneficiaries of their decisions.

215. Furthermore, it should be noted that only 3 out of the 37 members of the Management Committee have a non-technical professional background. Given that it consists primarily of information and/or technical officers, the Committee risks providing a rather technically biased perspective of the overall management of UNICC. In the view of the Inspectors, a more diverse membership in terms of professional background and orientation could provide a comprehensive view of the organizational and business aspects of UNICC strategy and operations, enabling it to better serve partner organizations. The Inspectors believe that the management of UNICC needs to develop a focus on the strategic and digital transformation of the United Nations system as a whole. Another issue reported by officers interviewed, and closely related to the composition of the Committee, is the limited access of UNICC to other, non-technical stakeholders in partner organizations. The ability to communicate more easily with other management structures inside partner organizations could be useful for defining possible common goals and strategies.

216. **The Inspectors recommend partner organizations of UNICC to ensure that it receives the strategic guidance needed for its repositioning. This could be achieved through, inter alia, the revision of the composition of the Management Committee to incorporate senior management members with a wide strategic vision in order to focus on the digital transformation of the United Nations system as a whole. Alternatively, guidance could be provided through other means, such as specific advisory groups and the Digital and Technology Network.** The Management Committee should continue to receive the appropriate technical support to allow informed decision-making by its members.

217. The Inspectors agree with the following views expressed by WIPO in its comments on the draft JIU report: “UNICC would benefit from a review and update of its mandate and membership. This would allow for a more in-depth evaluation of the financial and other resource implications of changing the mandate, as well as consideration of the appropriate balance of responsibilities between UNICC and the United Nations organizations.”

Recommendation 5

The General Assembly should review and update the mandate of UNICC, and consider, inter alia, diversifying the membership of the UNICC Management Committee and delegating appropriate levels of authority with respect to decision-making on digital information technologies, including cloud computing initiatives.

C. Services provided by the United Nations International Computing Centre

218. The cloud-related services currently offered by UNICC are given in box 8 below.

Box 8

UNICC cloud-related services

Client services:

- ICC consulting services
- Information technology advisory firm services
- Learning
- Monitoring

United Nations system private cloud solutions:

- SaaS: Unified communications (Enterprise Communications Service – ECS 2013)
- PaaS: ERP, enterprise web applications (hosting and traffic analysis), Enterprise SharePoint, business intelligence and database
- IaaS: Computing infrastructure (servers, storage and backup) and network infrastructure (network, Internet connectivity and OneICTBox)

Public cloud solutions:

- Integration and support: ECS Microsoft Office 365 Cloud, Microsoft Azure, AWS and cloud administration and support

Information security services:

- Common Secure
- CISO (Chief Information Security Officer) as a Service
- Information security operations

219. Data and information security is one major challenge faced by all organizations using cloud computing. The Inspectors believe that it would make sense to have a comprehensive United Nations system-wide approach to information security. In their view, this cannot be accomplished without the contribution and coordinated use of UNICC, which already offers security services and is actively working on further expanding its cybersecurity services. Cybersecurity is not only a technical matter: effective security today depends on trust, information-sharing and collaboration. UNICC is well positioned to foster collaboration and a community approach to cloud security matters among partner organizations. According to the officers interviewed, this is the fastest growing area of their services, with increasing acceptance among client organizations.

220. UNICC offers assistance with the security of data and applications in the cloud, regardless of the cloud service provider that the organization is using. Its services are complementary to the cloud security services of public providers, and offer an additional level of governance of cloud assets, particularly necessary for smaller organizations.

221. UNICC security services take into account the specifics of the United Nations system and offer a platform that promotes a safe environment for sharing security information within the community of their clients, an approach that is not entirely possible in the commercial sector and of particular interest to United Nations organizations. Thanks to the information-sharing among its clients, UNICC is able to detect certain threats that commercial providers cannot.

222. UNICC reduces the cost of access to threat intelligence, tracking and other important information services by obtaining umbrella agreements with commercial providers and sharing the cost of these services among their clients. It has similar arrangements with security companies.

223. Another example of economies of scale may be the joint undertaking of information security awareness campaigns. All organizations need to raise awareness among staff and keep them updated on the proper use of information, including associated technologies. UNICC has developed information security awareness and training materials tailored to the United Nations context that can be shared with different organizations, which is more efficient than if the materials were developed by each organization individually.

224. UNICC maintains a pool of consultants that are shared by clients. This is particularly useful for smaller organizations, whose needs vary and cannot justify maintaining a regular and highly skilled workforce, but it is equally beneficial for larger organizations as they also experience fluctuations in the demand for this type of service. Hiring high-quality information security professionals has become difficult today, and a concentrated hub approach may help overcome that particular challenge.

D. Unrealized potential and an opportunity for enhanced cooperation

225. Despite the system-wide vocation of UNICC, its potential has not been fully explored and realized. In its recent report to the General Assembly, the Advisory Committee on Administrative and Budgetary Questions expressed its continuing concern at the slow progress in reducing the level of fragmentation of the ICT landscape of the United Nations (A/73/759, para. 27). While the Advisory Committee was referring mainly to the Secretariat, the assertion is all the more valid for the United Nations system as a whole.

226. Many factors discussed in the present review point to opportunities for furthering cooperation in the context of more strategic and coordinated use of ICT resources by United Nations organizations. The Inspectors believe that UNICC could and should be one of the pillars supporting the digital transition, including the use of cloud computing. In fact, the characteristics inherent to cloud computing are conducive to the implementation of the UNICC mandate as the ICT shared services provider of the United Nations system.

227. UNICC holds unrealized potential as the strategic United Nations hub for supplying third-party public cloud services to partner organizations. Joint access to public cloud services could provide further cost savings, from a system-wide perspective, and leverage negotiation capacity.

228. UNICC could offer additional opportunities in its potential role as a cybersecurity hub for partner organizations to make their use of cloud services safer and their emergency response more effective. While security services are already offered by UNICC and its fastest growing services, there is still potential for bigger gains in this area, for the system as a whole, if more organizations join the hub. A number of security services become more effective when there are more participants sharing information and collaborating on data and application security.

229. In addition, UNICC offers significant potential for sharing and reusing market, service and technical intelligence with partner organizations, avoiding duplication of effort and making it easier for them to navigate the complicated and fast-changing range of services offered by commercial providers.

230. Furthermore, partner organizations that move part of their internal processing capacity to the public cloud often need to keep a remaining part of their ICT resources, including data, in their own data centres, for reasons including data sensitivity. This impacts the operations of data centres, which become partly used and over-dimensioned for the new needs, thus cost-inefficient. UNICC is in a position to provide managed or private cloud services for the sensitive portion of data and help partner organizations towards the implementation of cost-efficient hybrid solutions.

231. However, the Inspectors realize that the potential new role of UNICC needs to be carefully balanced, taking into consideration that a special and protected role for UNICC might reduce incentives for constant improvement of its services and economic efficiency. A centralized hub serving the whole community may also reduce the diversity of approaches, leading to a number of undesired consequences, including a slowdown in innovation. In order to realize the above potential benefits, there are some conditions that need to be addressed for UNICC to play a further role, by providing cloud and other shared ICT services to partner organizations in the United Nations system. **The Inspectors are of the opinion that there are at least three prerequisites in order to maximize the potential of UNICC as a system-wide service provider:**

(a) An operational mechanism that rewards internal efficiency and savings;

(b) A funding mechanism for research and development that could be linked to the achievement of internal efficiency and savings;

(c) Strong leadership and ability to persuade partner organizations' leadership to work together towards a joint vision of the digital future of the United Nations system.

232. There is a need for agreement and strong commitment from the leadership of partner organizations to guide UNICC towards a stronger role as the provider of shared ICT services to the United Nations system.

Annex I

A case study: Universal Postal Union as a cloud service provider

Highlights

1. The highlights of the case study are as follows:

(a) United Nations organizations are not only users of cloud services, but, in some cases, also providers;

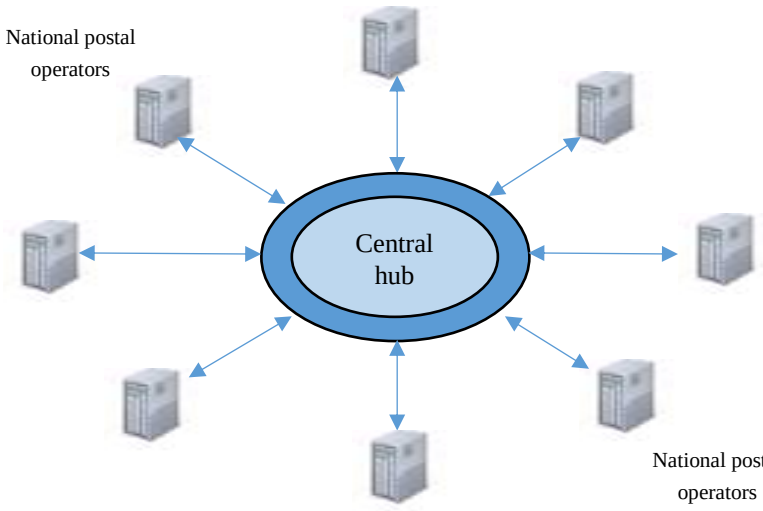
(b) UPU provides a cloud-based service (SaaS) to its members' national postal services;

(c) The service illustrates the ability of a United Nations specialized agency to design and operate a modern cloud-based service for the benefit of its stakeholders, respecting privacy and including the international legal protection of their data.

Background

2. UPU is one of the oldest international organizations and has been a United Nations specialized agency since 1948. As part of its mandate, UPU helps national post services to modernize and connect in order, inter alia, to provide end-to-end tracking of postal items. UPU activities in the parcels sector are focused on the provision of full-service international postal item products, with consistent end-to-end delivery times and strong customer support: for this purpose, UPU has developed a cloud-based application (SaaS).

Figure A.I
International tracking of postal items: traditional configuration



3. UPU has been developing and maintaining this software application since 1996, to facilitate international tracking of postal items by national post operators. Before this application was launched, national post operators were required to develop their own local solutions and interfaces for the global database maintained by UPU, using their local resources, including data centres, associated cybersecurity and networking. Each local copy handling national traffic had to connect to the global database, ensuring the synchronization of information (see figure A.I). This traditional model meant that each national postal operator also needed to test and deploy regular software updates that were necessary for modernization. The high level of effort and resources needed to keep up to date with the latest releases sometimes meant that national operators fell behind and failed to obtain the latest software version available and the features that it offered.

Introduction of a new cloud-based service

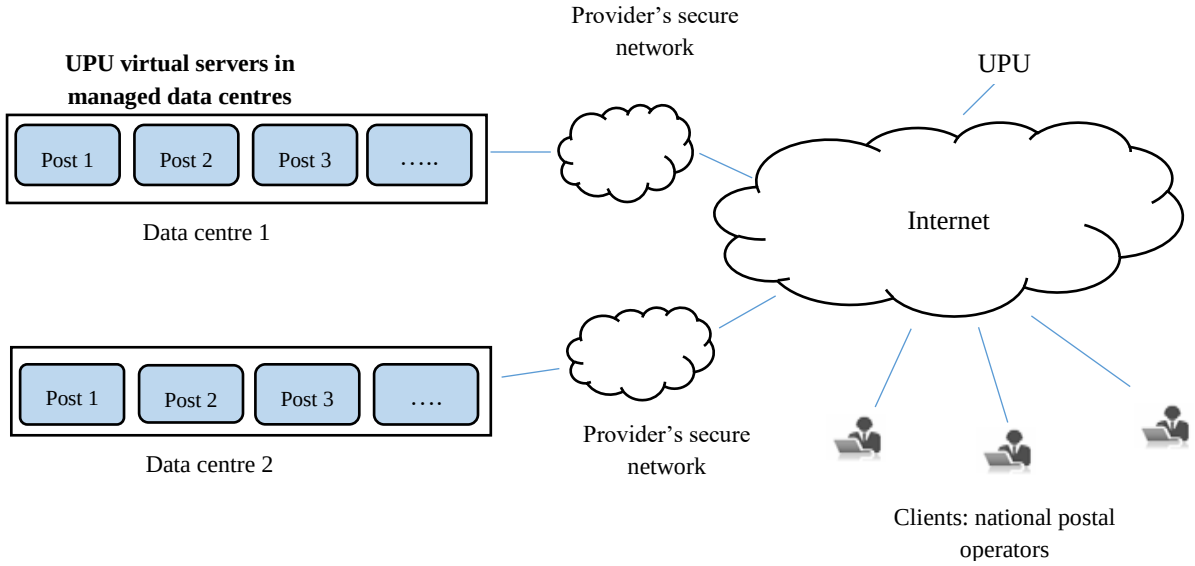
4. Based on feedback from the national postal services, UPU decided to develop and offer an application as a cloud-based service, in parallel with the traditional software package, offering member organizations a choice between the two models. With the cloud-based version of this service, the national operators do not have to install and run their own local versions of the database and the application: instead, they fully rely on their version in the cloud, created and maintained by UPU.

5. As described in figure A.II, UPU built a virtualized server infrastructure hosted by one of the biggest Swiss electronic communications providers. In doing so, UPU followed the highest industry norms for a robust and secure cloud infrastructure, with full redundancy, based in two geographically separated data centres. To ensure the highest level of information security, UPU follows standard ISO/IEC 27001 and is working (with UNICC) to obtain formal certification.

6. UPU charges its member organizations for the cloud-based service on a cost-recovery basis, distributing the cost of its cloud infrastructure among the clients.

7. In developing this solution, UPU took a conscious decision not to use the infrastructure of the largest commercial public cloud providers. Its decision was to locate the infrastructure and the data that it hosts in the same country the UPU headquarters, under a jurisdiction that fully respects United Nations privileges and immunities, and to work with a local communications provider. UPU considers the network accessibility security and protection offered through this provider to be adequate for the needs of the system that it operates.

Figure A.II
New cloud-based service



Benefits

8. The benefits provided of the UPU cloud SaaS application are as follows:

(a) From the perspective of the individual clients (national post operators), it involves a significant reduction in the cost and complexity of operating the system locally, as there is no local computing infrastructure to purchase and maintain. Compared to the older system, the savings arise not only from sharing the infrastructure, but also from sharing the skill set and competencies that UPU has developed and maintains in order to run the system;

(b) Clients are always up to date, using the latest version of the application, as they use the software provided directly by UPU through the Internet;

(c) Support on the application is much faster;

(d) This solution also enables faster data exchange than under the previous configuration.

Annex II

Overview of the current use of cloud computing services in the United Nations system

Contents

	FAO	IAEA	ICAO	ILO
Service model	IaaS, PaaS, SaaS	IaaS, PaaS, SaaS	IaaS, SaaS	IaaS, PaaS, SaaS
Cloud strategy/policy	Part of a digital strategy (not provided) for ERP, technical platforms, etc. Contractual clause.	Enterprise architecture guidelines. Cloud guidance (user reference).	Drafting to integrate cloud strategy into its global information technology strategy.	Cloud-first assumed, currently drafting a formal strategy.
Data strategy/policy	Data classification policy (AC 2013/23 and MS505 (2013)). Data sets individually assessed for migration to the cloud.	Administrative manual, part II, section 19 ("Information security").	Administrative Instructions on Information Classification and Handling (June 2009).	Classification of ILO Information Assets (IGDS No. 456, January 2016). No general restrictions; data are assessed on a case-by-case basis for moving to the cloud.
Deployment model	Public, hybrid, private (planning stage)	Hybrid	Public, hybrid, private, community	Public, private
United Nations privileges and immunities	Preserved by choosing data locations/jurisdictions in which United Nations privileges and immunities are recognized and respected. Unclear how providers can fully comply with them in the public cloud.	Preserved through references in contractual clauses, requirement that data be stored within Europe.	Only fully assured by UNICC services.	Specified in contractual terms, including control over data location.
Expected/targeted benefits or motivation	• Agility • Security • Transparent costing • Best practices, information technology standards • Scalability • Innovation • Software standardization	• Simplification (reducing low-level infrastructure) • Improved business continuity and disaster recovery • Security • Faster deployment • Continuous evolution	• High availability • Flexibility • Access to innovation • Modernization • Self-service • Broad network access • Elasticity • Resource-pooling	• Reduce capital investment • 24/7 support • Multiplatform support • Delegate maintenance complexity to vendors • Better security • Overcome in-house skills gap • Latest functionality available
UNICC services used	• ERP, other applications hosted • Consulting	• ERP • Information security	• Federated authentication • Information security	• Disaster recovery hosting • Email hosting • Microsoft SharePoint hosting • Skype for Business hosting • Information security

	IMO	ITC	United Nations Secretariat	UNDP
Service model	IaaS; SaaS is under consideration	IaaS, SaaS; PaaS under consideration	IaaS, PaaS, SaaS	IaaS, PaaS, SaaS
Cloud strategy/policy	Internal memorandum on data classification, data management, cloud computing and use of computers (February 2015), informed by United Nations system discussion and envisaging UNICC as the United Nations community cloud. Currently under review.	Using United Nations Secretariat's policy.	United Nations Secretariat cloud strategy (April 2018); Cloud computing: United Nations Secretariat ICT technical procedure (INF.09.PROC., March 2017).	Engineering best practices.
Data strategy/policy	Data classification and management policy (June 2015).	Using United Nations Secretariat's policy.	Secretary-General's bulletin on information sensitivity, classification and handling (ST/SGB/2007/6, February 2007).	Information classification and handling guidelines (unknown date).
Deployment model	Hybrid	Public	Public, private, hybrid	Public
United Nations privileges and immunities	The contract covers United Nations privileges and immunities. Data centre located in the United Kingdom of Great Britain and Northern Ireland.	Legal opinion sought for customer relationship management.	Vendor's privacy and security provisions in a separate document, as a supplement to its services terms and conditions. Negotiated with the assistance of OLA. The service provider accepts the status of United Nations data as United Nations archives, but recognizes the reality of multi-tenant infrastructure and shared resources. OLA advised that highly confidential data should be internally managed.	Contractual provisions. For Microsoft Office 365, UNDP has chosen the data centre in Ireland to ensure that UNDP data falls under the jurisdiction of European Union privacy laws.
Expected/targeted benefits	• Elasticity, resource pooling • Cost-efficiency • Analytics	• Future-readiness • Cost-efficiency • Scalability • Speed • Resource optimization • Cloud-based features	• Agility • Cost savings • Innovation opportunities	• Security • Performance (-to-price ratio) • Resource elasticity • Lower cost of ownership
UNICC services used	• Disaster recovery and business continuity • Security (planned) • Cloud computing consulting (planned)	• Non-cloud services only • Information security	• Disaster recovery hosting • Email hosting • Microsoft SharePoint hosting • Skype for Business hosting • Application development and support • Network support	• ERP hosting services (conventional) • Hosting legacy web applications • Microsoft SharePoint hosting • Information security

	UNEP	UNESCO	UNFPA	UNHCR
Service model	IaaS, SaaS	IaaS, PaaS, SaaS	IaaS, SaaS	IaaS, PaaS, SaaS
Cloud strategy/policy	Aligned with the United Nations OICT strategy. United Nations Secretariat cloud strategy (April 2018); Cloud computing: United Nations Secretariat ICT technical procedure (INF.09.PROC., March 2017); Relying on the contingency plans of the United Nations Office at Nairobi (UNON) and CloudVPS for business continuity.	No formal strategy. Decisions guided by the United Nations Legal Advisors Network on risk assessment.	The 2018–2021 ICT strategy for UNFPA recommends cloud use, without specifying an explicit cloud computing strategy. Organizational business continuity plans rely on Google cloud services.	No cloud-specific policy.
Data strategy/policy	Secretary-General's bulletin on information sensitivity, classification and handling (ST/SGB/2007/6, February 2007).	Information sensitivity classification standard.	Policy and procedures for document management at UNFPA (May 2018); Policy for information disclosure (June 2009).	Policy on the protection of personal data of persons of concern to UNHCR (November 2015).
Deployment model	Public, private	public	Public	Public, community
United Nations privileges and immunities	UNON-hosted services are Nairobi-based. CloudVPS data centres are in the Netherlands. Microsoft Office 365 tenancy is with the United Nations OICT.	Granted for Office 365 (joint contract with other United Nations agencies), using data centres in Ireland (moving to France in the future). European data centres chosen for Cornerstone and Taleo. No specific provisions for smaller SaaS (such as Everbridge).	Contractual clause specifies provider's good faith effort to respect legal process related to the United Nations privileges and immunities. No control over geographical location of data in the cloud and their jurisdiction.	Contractual provisions (approved by the United Nations legal office) for Microsoft and Amazon agreements.
Expected/targeted benefits or motivation	• Cost-efficiency • High availability • Flexibility • Scalability • Reduced maintenance workload • Quality of service • Automation • Elasticity • Ease of use	• Premium functionality available with cloud-based solutions only (for example, human resources management) • Global availability of Office 365 • Future functionality improvements available with cloud-based solutions • Elasticity • Reduced complexity of ICT operations	• Reduced complexity of ICT operations • Standardization • Flexibility and scalability	• Flexibility • Agility • Refocusing of internal resources on core-business ICT • Wide global access
UNICC services used	None	• Disaster recovery • Gartner • CISO-as-a-Service, Common Secure • Information security	Using Atlas, hosted by UNICC and managed by UNDP.	• PeopleSoft ERP hosting • Consultation of UNICC on cybersecurity, Office 365 and Azure Active Directory for its extensive knowledge.

	UNICEF	UNOPS	UNOV/UNODC	UNRWA
Service model	IaaS, PaaS, SaaS	IaaS, PaaS, SaaS	SaaS	IaaS, SaaS
Cloud strategy/policy	UNICEF guidance on public cloud services provisioning (October 2016); From the data centre to the cloud: UNICEF hosting strategy (September 2016).	High-level ICT 2018 goals.	Cloud computing: United Nations Secretariat ICT technical procedure (INF.09.PROC., March 2017); Use of cloud computing in the United Nations system: recommendations for risk mitigation (June 2013);	IT Strategy "Information Management Department Strategy 2019-2020".
Data strategy/policy	UNICEF Standard On Information Security: Asset Management (January 2018).	Document retention policy (to be received).	Secretary-General's bulletin on information sensitivity, classification and handling (ST/SGB/2007/6, February 2007). No general restrictions, data are assessed on a case-by-case basis for moving to the cloud.	Information security policy (February 2011); does not explicitly deal with cloud storage of data.
Deployment model	Public	Public	Public, private	Hybrid
United Nations privileges and immunities	Ensured through contractual provisions, including data location choice.	Included in the legal agreement with the vendor. UNOPS has control over location of data for application hosting. Encryption ensured through customer-supplied and customer-managed encryption keys.	Specified in contractual terms, including control over data location.	• The UNRWA general conditions of contract for the provision of services apply to public cloud services with specific contracts • United Nations Global Service Centre services: fully compliant • Salesforce (free) default contract applies; data location and conditions not clear
Expected/targeted benefits or motivation	• Cost-efficiency • Increased technical options • Innovation opportunities • Agility	• Global reach, bandwidth, accessibility • Resilience • Enhanced remote collaboration • Access to innovation	• Alignment with United Nations Secretariat and its policies	• Location of critical system and services to a safe location (outside the agency location) • Minimal staff requirement • Speed of deployment • Up-to-date infrastructure • Use of mature information technology processes • Cost-efficiency • Accessibility • High service availability
UNICC services used	• Professional services on information technology security	None. Needs the global network reach of large public cloud providers.	• Common Secure (non-subscriber version)	• SAP technical operations services • Advisory services

	UN-Women	UNWTO	WFP
Service model	IaaS, PaaS, SaaS	IaaS	IaaS, PaaS, SaaS
Cloud strategy/policy	UN-Women information technology strategy specifies a cloud-first strategy, with a view to adoption of an SaaS-first strategy in the future.	Under development.	Corporate information technology strategy (2016–2020); WFP cloud computing position paper (2014) (under review).
Data strategy/policy	Data classification policy (unspecified).	Draft ShareFile policy (2015).	Directive on records retention policy in WFP (AD2006/006); Directive on information disclosure (CP2010/001); Corporate information and information technology security policy (OED2015/012) (all are under review).
Deployment model	Public, community	Public	Public, private, community
United Nations privileges and immunities	Ensured through contractual provisions with vendors. UN-Women controls data location.	Using European data centre locations.	Contractual provisions in line with inter-unit jointly developed conditions and input from OLA.
Expected/targeted benefits or motivation	• Cost-efficiency • Broader feature set • Productivity gains from better global access and collaboration • All the standard cloud benefits	Provision of a secure consolidated service as an alternative to spontaneous individual use of the cloud by staff (file-sharing).	• Keeping up with the changing needs of the Organization • Financial benefits/cost savings • Risk optimization • Service quality
UNICC services used	Professional services, completing public cloud, infrastructure monitoring, cloud tenant management and administration, information security and reporting.	None	• Data centre management (onsite and remote) • Storage (Storage Area Network) • Database administration • ERP administration • Microsoft Office 365 administration, including email and SharePoint • Information technology security services

	WHO	WIPO	WMO
Service model	IaaS, PaaS, SaaS	IaaS, PaaS, SaaS	SaaS
Cloud strategy/policy	Cloud computing policy (November 2015).	Cloud services policy (May 2018): defines a cloud-first strategy. Business continuity policies: referred to when using cloud services.	None
Data strategy/policy	Information classification policy.	Information security classification and handling policy with four levels of security classification. No restrictions on hosting data in the cloud.	None
Deployment model	Public, private, community	Public, hybrid (transitional), private (future)	Public
United Nations privileges and immunities	Contractual clauses, with control over data location (Europe).	Covered by contractual provisions. Full control over data location for IaaS and PaaS.	Not safeguarded. No control over data location.
Expected/targeted benefits or motivation	• Cost savings • Performance improvements • Security • Agility • Scalability and elasticity • Innovation • Self-service • Geographical distribution • Business enabling innovative solutions • Improved disaster recovery • Business continuity • Broad network access • Resource pooling • Data centres	• Cost optimization • Agility and flexibility • Efficient service delivery • Improved business continuity • Generic cloud computing benefits	Unknown due to changes in the information technology team
UNICC services used	• ERP • Business intelligence • SharePoint • Information security • Managed hosting • Application development	• Email • Network services • ICT service management • ICT application hosting • Network support	Hosting, managed and professional services, information security

Supplier	Product	FAO	IAEA	ICAO	ILO	IMO	ITC	Secretariat	UNDP	UNEP	UNESCO	UNFPA	UNHCR	UNICEF	UNOPS	UNOV/UNODC	UNRWA	UN-Women	UNWTO	WFP	WHO	WIPO	WMO
Adobe	Connect			✓		✓														✓			
Amazon	AWS	✓	✓	✓			✓	✓					✓	✓				✓	✓	✓	✓	✓	
Atos (remote hosting)	Oracle ERP hosting				✓																		
BeDataDriven	ActivityInfo																✓						
Cisco	IronPort	✓																					
CloudSigma	Infrastructure hosting																					✓	
CloudVPS	Public website hosting									✓													
Cornerstone	Human resources management, talent management, learning										✓												
Cornerstone	Learning management system										✓										✓		
Cornerstone	Performance management and e-learning	✓					✓				✓												
Corporater	Business management platform																						
CrossKnowledge	E-learning																	✓		✓			
Cvent	Event management	✓																					
Dell	Red Cloak			✓																			
DocuSign	Electronic signatures and contracts																						
Dropbox	Cloud-based data storage and sharing				✓																		
Everbridge	Critical event management										✓												
FleetWave	Fleet management																			✓			
Fluxx	Grantmaker																						
Form.io	Forms and data management																						

Supplier	Product	FAO	IAEA	ICAO	ILO	IMO	ITC	Secretariat	UNDP	UNEP	UNESCO	UNFPA	UNHCR	UNICEF	UNOPS	UNOV/UNODC	UNRWA	UN-Women	UNWTO	WFP	WHO	WIPO	WMO
Google	(Unspecified)	✓																					
Google	Google Cloud Platform (application hosting)											✓			✓								
Google	G Suite											✓			✓								✓
Google	Gmail											✓											
Imperva	Web Application Firewall	✓																					
In-tend	Procurement sourcing	✓																					
Kyriba	-																						
Lynda	Online courses																				✓	✓	
McAfee	Antivirus software				✓																		
Medgate/Cority	Environmental health, safety and quality software																			✓			
Medgate/Cority	Health care												✓										
Microsoft	Azure Storage		✓	✓		✓	✓	✓	✓	✓	✓		✓	✓				✓		✓	✓	✓	
Microsoft	Dynamics						✓				✓												
Microsoft	Azure Functions																	✓					
Microsoft	Intune					✓								✓				✓					
Microsoft	Office 365	✓	✓			✓		✓	✓	✓	✓		✓	✓		✓	✓	✓		✓	✓		
Microsoft	OneDrive					✓	✓				✓					✓		✓			✓		
Microsoft	Azure Cache for Redis																	✓					
Microsoft	SharePoint					✓			✓		✓							✓			✓		
Microsoft	Skype					✓										✓		✓					

Supplier	Product	FAO	IAEA	ICAO	ILO	IMO	ITC	Secretariat	UNDP	UNEP	UNESCO	UNFPA	UNHCR	UNICEF	UNOPS	UNOV/UNODC	UNRWA	UN-Women	UNWTO	WFP	WHO	WIPO	WMO
Microsoft	System Center Configuration Manager	✓				✓																	
Microsoft	Web Apps					✓												✓			✓		
Microsoft	Web Jobs																	✓					
Okta	-																						
Oracle	Financing reporting				✓																		
Oracle	Human resources																	✓					
Oracle	Learning management								✓														
Oracle	Performance management								✓														
Oracle	Taleo	✓	✓								✓	✓						✓			✓		
Others	-		✓																				
Salesforce	Customer relationship management											✓	✓				✓	✓		✓			
SAP	E-Recruiting				✓															✓			
SAP	Learning management				✓																		
SAP	Performance management				✓																		
SAP	SuccessFactors				✓						✓									✓			
SAP	Talent Management				✓																		
ServiceNow	Information technology services, security (implied)												✓					✓			✓		

Supplier	Product	FAO	IAEA	ICAO	ILO	IMO	ITC	Secretariat	UNDP	UNEP	UNESCO	UNFPA	UNHCR	UNICEF	UNOPS	UNOV/UNODC	UNRWA	UN-Women	UNWTO	WFP	WHO	WIPO	WMO
SurveyMonkey	-	✓				✓					✓							✓					
Tableau	-						✓															✓	
TakeFlight	Airline enterprise software solution																			✓			
UNDP	ERP											✓						✓					
UNICC	Application hosting	✓	✓			✓	✓		✓				✓					✓			✓	✓	✓
UNICC	Common Secure (information security)		✓	✓	✓	✓	✓		✓		✓		✓	✓		✓	✓	✓		✓	✓		✓
UNICC	Disaster recovery (hosted)				✓	✓			✓		✓		✓					✓				✓	
UNICC	Federated authentication/ Common Connect			✓					✓			✓										✓	
UNICC	Microsoft SharePoint (hosted)				✓				✓												✓		✓
UNICC	Outlook email (hosted)				✓		✓															✓	
UNICC	PeopleSoft/SAP / e-Business ERP hosting or support	✓	✓						✓			✓	✓				✓	✓				✓	
UNICC	Private cloud					✓														✓			
UNICC	Skype for Business (hosted)				✓		✓															✓	
UNICC	Support in the public cloud												✓	✓				✓		✓			

UNICC	Network support and connectivity								✓									✓				✓	✓
UNICC	Application/business intelligence development and support	✓					✓	✓	✓				✓										
Unit4	E-recruitment			✓																			
United Nations Global Service Centre	Hosting									✓							✓						
United Nations Secretariat	Inspira									✓						✓							
United Nations Secretariat	Umoja						✓			✓						✓							
UNON	Infrastructure hosting					✓				✓													
Unspecified	Recruitment																					✓	

Annex III

Overview of actions to be taken by participating organizations on the recommendations of JIU

JIU/REP/2019/5

		Intended impact	CEB	United Nations and its funds and programmes															Specialized agencies and IAEA											
				United Nations*	UNAIDS	UNCTAD	ITC	UNDP	UNEP	UNFPA	UN-Habitat	UNHCR	UNICEF	UNODC	UNOPS	UNRWA	UN-Women	WFP	FAO	IAEA	ICAO	ILO	IMO	ITU	UNESCO	UNIDO	UNWTO	UPU	WHO	WIPO	WMO
Report	For action		☐	☒	☒	☒	☐	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
	For information		☒	☐	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Recommendation 1		e		E	E	E		E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E
Recommendation 2		f h		L	L	L		L	L	L	L		L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L
Recommendation 3		f h		E	E	E		E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E
Recommendation 4		g h		E	E	E		E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E
Recommendation 5		f h		L																										

Legend: **L:** Recommendation for decision by legislative organ **E:** Recommendation for action by executive head

: Recommendation does not require action by this organization

Intended impact: **a:** enhanced transparency and accountability **b:** dissemination of good/best practices **c:** enhanced coordination and cooperation **d:** strengthened coherence and harmonization **e:** enhanced control and compliance **f:** enhanced effectiveness **g:** significant financial savings **h:** enhanced efficiency **i:** other.

* As listed in ST/SGB/2015/3.