|  |  |
| --- | --- |
| **Council Working Group on Financial and Human Resources****Fourteenth meeting – Virtual, 20 – 21 September 2021** |  |
|  |  |
|  | **Document CWG-FHR-14/10** |
| **19 August 2021** |
| **English only** |
| **Contribution by the Secretariat** |
| Update on UMACs Item A: ITU - Business Continuity and Information Management |

|  |
| --- |
| SummaryDuring C21/VCC-1 Member States discussed document [C21/49](https://www.itu.int/md/S21-CL-C-0049/en) (List of 2021-2027 unfunded mandatory activities) and *instructed the secretariat to present the implementation of these requests as well as other unfunded mandatory activities outlined in Table 1 of document C21/49 planned for the 2021-2027 time-frame to the next CWG-FHR session in September 2021 and the next Council sessions (*see line 20 ofANNEX 1 of letter [DM-21/1017](https://www.itu.int/md/S21-DM-CIR-01017/en) on the Results of the consultation on outcomes of discussions of the 2021 Virtual consultation of councillors (C21/VCC-1), 8-18 June)*.* See also line 26 on an Organizational Resilience Management System (ORMS), also relevant to business continuity and information management.Table 1 of document C21/49 provided estimates for 2021-2027 for UMACs and included Item A: ITU – Business Continuity and Information Management (CWG-FHR-12/3 and C20/53) requesting CHF 13 million over the same period. This document presents to CWG-FHR and CWG-SFP additional information related to Item A, namely, the need for strengthening digital asset management, as highlighted in the PwC forensic report, a recommendation by the JIU in the form of a management letter, and an extract from document CWG-FHR-14/INF1 on the proposed strengthening of the ITU accountability framework, and ORMS.Action requiredBased upon the Council 21 decisions mentioned above on UMACs and ORMS, and the additional information presented in this document, the CWG-FHR is invited **to advise** on the funding for the implementation of Item A - ITU Business Continuity and Information Management.\_\_\_\_\_\_\_\_\_\_\_\_References*Council documents* [*C20/53*](https://www.itu.int/md/S20-CL-C-0053/en) *(Business Continuity and Information Management)*,[*C20/74*](https://www.itu.int/md/S20-CL-C-0074/en) *(PwC report),* [*C21/15*](https://www.itu.int/md/S21-CL-C-0015/en) *(Organizational Resilience Management System (ORMS)), and* [*C21/49*](https://www.itu.int/md/S21-CL-C-0049/en)*(List of 2021-2027 unfunded mandatory activities (UMACs)); Council Working Group on FHR documents* [*CWG-FHR-12/3*](https://www.itu.int/md/S21-CWGFHR12-C-0003/en) *(Business Continuity and Information Management),* [*CWG-FHR-14/2*](https://www.itu.int/md/S21-CWGFHR14-C-0002/en) *(Strengthening the ITU accountability framework,) and the description in* [*CWG-FHR-14/INF1*](https://www.itu.int/md/S21-CWGFHR14-INF-0001/en)*. Letter* [*DM-21/1017*](https://www.itu.int/md/S21-DM-CIR-01017/en) *on the Results of the consultation by correspondence on the outcomes of discussions of C21/VCC-1. JIU/ML/2021/X “Management letter on securing the integrity of documents, records and archives of the United Nations system organizations” (*[*Annex 1*](#Annex1)*).* |

**Background**

During the VCC-21 Member States discussed document C21/49 UMACs and instructed the secretariat to present the implementation of these requests as well as other unfunded mandatory activities outlined in Table 1 of document C21/49 planned for the 2021-2027 time-frame to the next CWG-FHR session in September 2021 and the next Council sessions.

Implementation of UMAC Item A: ITU – Business Continuity and Information Management (CWG-FHR-12/3 and C20/53) requires an estimated CHF 13 million over the period 2021-2027.

**Additional information**

CWG-FHR and CWG-SFP should be aware of the following additional information in the PwC forensic report, the JIU management letter, the proposed strengthening of the ITU accountability framework and the ORMS approval.

1) PwC forensic report recommendations 62-69 on ***Forensic investigation readiness and data management*** and the ITU SG acceptance (doc xxx) with the following caveats:

*they require development of a comprehensive ITU-wide organizational governance and compliance framework as a pre-requisite to subsequently implementing adequate technical solutions to support the policies and procedures; 2017-2027 (Doc C20/53) Timelines for implementation of technical solutions will be identified after approval of policies and procedures; CHF 13 mill (Doc. C20/53) pending Council approval; Developing a governance framework is an organization-wide effort not limited to ISD; Additional resources required for implementation of technical solutions will be identified after approval of policies and procedures.*

2) JIU management letter (JIU/ML/2021/X) in which the JIU recommend:

*The Inspectors request the executive heads of the Joint Inspection Unit participating organizations to give urgent consideration to devising and applying heightened safeguards to secure their current and historical documents, records and archives, including by revisiting the security parameters applied to the storage of such documents in both the physical and cyber-environment and including the matter in their organizations’ risk registry, and to report to the Joint Inspection Unit no later than the end of 2021 on the steps taken to address the risk.*

The Inspectors believe it prudent to bring this matter in the form of a Management Letter to the attention of the executive heads of all participating organizations, for action as appropriate

3) Strengthening the ITU accountability framework (CWG-FHR14/2 para 25, CWG-FHR-14/INF-1):

*The need for a* ***Legal and Compliance Framework of Digital Assets*** *has also been identified. Consequently, information assets need to be protected from loss, damage, or unauthorized disclosure or modification. At the same time, data protection and data privacy are becoming a priority, requiring policies, procedures, and systems to ensure that personal information is captured, stored, and processed in ways that are secure. To address these concerns, ITU is developing an organization-wide data/information classification framework that includes classifying information in terms of both its need for protection from unauthorized access or disclosure (sensitivity) and its need for availability (criticality), and identifying and implementing the protection requirements for each category of information (both sensitivity and criticality) throughout the information lifecycle (creation, storage, use, and disposal).*

*In parallel with the rapid rollout of tools to enable staff and delegates to work remotely, ITU accelerated the establishment of* ***information governance frameworks*** *adapted to fully digital work processes. ITU corporate systems (e.g., SAP ERP, CRM, Recruitment) are being upgraded not only to ensure continuing vendor support but also to benefit from improved or new functionalities related to data protection, information management compliance, and data analysis based on AI/Machine Learning. The issues of “Device acquisition procedures for forensic investigations” and “legal hold procedures” are being reviewed, and guidelines developed, in connection with the newly established investigation function*.

4) Council 21 approved the ORMS framework in C21/15 and noted *“..the request for a creation of a project to define an ITU Data Classification system as contained in the CWG-FHR report (C21/50+Add.1)*”, (see [ANNEX 1 - Results of the consultation on outcomes of discussions of the 2021 Virtual consultation of councillors (C21/VCC-1), 8-18 June](https://www.itu.int/md/S21-DM-CIR-01017/en)). This data classification system will be an integral part of business continuity and information management.

Action required:

Based upon the Council 21 decisions mentioned above on UMACs and ORMS, and the additional information presented in this document, the CWG-FHR is invited to advise on the funding for the implementation of Item A - ITU Business Continuity and Information Management.

ANNEX 1

**DRAFT**
JIU Management letter (JIU/ML/2021/X “Management letter on securing the integrity of documents, records and archives of the United Nations system organizations” )

I**NTRODUCTION**

1. The Joint Inspection Unit (JIU) included a report entitled *Cybersecurity in the United Nations system organizations: a review of policies and practices* as part of its 2020 Programme of Work in line with the objectives of the Strategic Framework of the Unit. The review is expected to provide insights for participating organizations to strengthen governance, enhance accountability, identify priority areas to improve overall cyber-resilience and to lower exposure to cyber-risks. During the preparation of the report, the Inspectors were informed of risks associated specifically with the safeguarding and protection of organizations’ legal, normative, administrative, political and historical documents and data. The Inspectors believe it prudent to bring this matter in the form of a Management Letter to the attention of the executive heads of all participating organizations, for action as appropriate.

**SECURING THE INTEGRITY OF DOCUMENTS, RECORDS AND ARCHIVES OF THE UNITED NATIONS SYSTEM ORGANIZATIONS**

1. The members of United Nations system organizations have vested in them a custodial role with respect to intergovernmental documents, which are often the product of protracted negotiation and sensitive diplomatic processes. These documents include, but are not limited to, treaties and conventions, parliamentary documents, information given into the organizations’ custody by their members, and information generated by the organizations themselves in fulfilling their respective mandates. If their content or any aspect of their articulation, including associated voting records, accompanying notes, chronological information, lists of participants, names or the functional capacities of persons reflected as participating in the documents’ creation, were altered, particularly retroactively and without being detected for extended periods of time, it could cause considerable damage to the point of endangering international safety and security. Similar considerations apply to administrative records which form the backbone ensuring the functioning of the respective organization and its ability to carry out its mandated activities. Whether such documents are stored in digital or paper form, and irrespective of whether they are archived and represent historical documentation or are in current use, possibly even subject to live debate, the protection of their integrity is undisputedly of paramount importance.
2. The “triad of information security” that encompasses the confidentiality, integrity and availability of information, including electronically stored data, highlights the essential characteristics of information that require protection, as defined with a view to focusing information holders’ commitment to safeguarding all information from both external and internal interference. While availability and confidentiality aspects already enjoy high visibility and prominence, the integrity of data, documentation and systems used to store them is less obvious and can be tampered with in dangerous and stealthy ways.
3. A JIU report on records and archives management[[1]](#footnote-1) issued in 2013 underlined the importance of protecting the physical and electronic environment where data is stored, limiting access to information that is considered confidential, restricted or secret and retaining and safeguarding all records considered to be of permanent value. It also highlighted inherent risks in terms of integrity, security and authenticity as digital records can potentially be easily modified, deleted and moved while users’ actions are difficult to trace appropriately. Replications are commonly performed without detection and controls to safeguard their integrity are limited.
4. United Nations system organizations have introduced a variety of digital systems to facilitate access to their records and archives, including to diplomatic delegations, governments, researchers and the wider public. These systems have eliminated some challenges, yet brought about others, including new risks associated with preserving the systems’ own authenticity, usability and integrity. The United Nations system organizations, on different occasions, stated that their ICT systems are facing increasing risks, as they are exposed to external and internal threats which are significant and growing in scale and complexity and further exacerbated by vulnerabilities related to lack of effective and efficient cybersecurity management and investment. These risks and challenges grow more critical as the volume of records, including those in digital format, increases. On the occasion of the preparation of the report on cybersecurity, the Inspectors received indications that this risk is not hypothetical but amounts to a real threat and confirmed that participating organizations have encountered difficulties of that kind.
5. Some effective preventive measures for preserving data integrity might be taken through the careful design of information systems architecture (for example using document checksums, digital signatures, change logs and similar techniques), but there is an acute need to address data integrity throughout the entire lifecycle of documents. As an emerging technological solution with data integrity in focus, distributed ledgers might also be studied by organizations for use in building tampering-resistant archives, since, technically, a record on a blockchain remains unchangeable after it has been created.[[2]](#footnote-2)
6. It is critical for organizations in the United Nations system as custodians of documents of global importance to ensure that they are secure and their integrity is protected against risks and threats, including cyber-risks. The Inspectors urge participating organizations to increase their attention to devising and applying heightened safeguards to secure their current and historical documents, records and archives, including by revisiting the security parameters applied to the storage of such documents in both the physical and cyber-environment with a view to maximally protecting them from being tampered with. The most appropriate controls to ensure the completeness, accuracy, consistency and reliability of information in this regard should be identified according to the level of protection required to match each organization’s own situation based on a dedicated risk assessment focusing on the integrity aspect of cybersecurity.

|  |
| --- |
| **Recommendation** **The Inspectors request the executive heads of the Joint Inspection Unit participating organizations to give urgent consideration to devising and applying heightened safeguards to secure their current and historical documents, records and archives, including by revisiting the security parameters applied to the storage of such documents in both the physical and cyber-environment and including the matter in their organizations’ risk registry, and to report to the Joint Inspection Unit no later than the end of 2021 on the steps taken to address the risk.**  |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. JIU/REP/2013/2: *Records and Archives Management in the United Nations*. [↑](#footnote-ref-1)
2. *Blockchain applications in the United Nations system: towards a state of readiness*, JIU/REP/2020/7, para. 142. [↑](#footnote-ref-2)