|  |  |
| --- | --- |
|  | **Document CWG-FHR-16/6** |
| **11 September 2023** |
| **English only** |
|  |  |
| Contribution by the secretariat |
| REPORT ON CYBERSECURITY FRAMEWORK AND INTERNAL CONTROLS WITHIN ITU |
| **Purpose**In its report on Cybersecurity in the United Nations system organizations ([JIU/REP/2021/3](https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_3_english.pdf)), the Joint Inspection Unit (JIU) recommended the executive heads of the United Nations system organizations to present a comprehensive report on their cybersecurity framework to their governing bodies, covering elements contributing to an improved cyber resiliency. This document aims to address the JIU recommendation by providing a comprehensive overview of the cybersecurity framework as currently implemented in ITU's network. It emphasizes the critical operational elements that ITU is employing holistically to enhance its cyber resiliency and preparedness for dealing with cyber incidents. It should be noted that the July session of Council 23 approved the recommendation of the Independent Management Advisory Committee (IMAC) to further strengthen the ITU cyber security posture ([C23/22](https://www.itu.int/md/S23-CL-C-0022/en) - IMAC Annual Report, and [C23/25](https://www.itu.int/md/S23-CL-C-0025/en)). Furthermore, the digital transformation document presented to council 23 included also references to strengthening cyber security services.**Action required**The CWG-FHR is invited to **consider** the report and **provide strategic guidance** on further improvements to be implemented (*2nd JIU recommendation*).\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**References**[JIU/REP/2021/3](https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_3_english.pdf):Cybersecurity in the United Nations system organizations[Council Document C23/22](https://www.itu.int/md/S23-CL-C-0022/en): Twelfth Report of the Independent Management Advisory Committee (IMAC) – Annual Report for 2022-2023[Council Document C23/25:](https://www.itu.int/md/S23-CL-C-0025/en) Strengthening ITU's Regional Presence |

**1. Background**

1.1 The increasing reliance of ITU on digital technology has brought about numerous benefits in accomplishing its mandate, but it has also created new vulnerabilities that can be exploited by cyber attackers. In today's interconnected world, the threats to cybersecurity are greater than ever, and they continue to evolve at an alarming pace. Cyber-attacks can disrupt ITU’s operations, its physical and virtual meetings, cause data loss/leakage, and damage its reputation. Over the course of the past decade, a framework for cybersecurity has been established, consisting of a range of procedures and technologies designed to safeguard ITU's information systems, networks, and data against unauthorized access, use, disclosure, disruption or destruction. This framework encompasses various elements, such as **cyber risk assessment, access control management, identity management, threat analysis, vulnerability management, security operations centre and cyber incident response.** Additionally, it includes regular training and awareness for staff, with regular phishing campaigns and activities, conducted to evaluate its effectiveness. The framework is aligned with leading industry standards like ITU-T recommendations, ISO27001 and frameworks such as COBIT, CIS and NIST.

1.2 ITU is using an external cybersecurity rating and risk-monitoring platform, which offers real-time insights and analysis of our security posture. The platform uses a letter-grade scale, ranging from "A" to "F," with "A" denoting the highest rating and "F" the lowest. Presently, ITU holds an "A" grade, placing ITU among the top agencies in comparison to others UN sister organizations. Despite not experiencing any significant cyber-attacks in the past decade, a high risk of a breach remains. Therefore, it is essential to maintain a strong cybersecurity posture and continue to improve our cyber resiliency and business continuity mitigation measures. Considering the fast-paced development of emerging cyber threats, there is a need for the framework to be enhanced to become more all-encompassing, adaptable, and consistently revised to address these new risks. It must not be seen as a separate activity, but rather fully incorporated into wider organizational endeavors, such as the **Organizational Resilience Management System** (**ORMS**[[1]](#footnote-1)**)**, enterprise risk management, **business continuity planning**, **digital asset management**, compliance framework, and information governance framework.

**2.** **Current state of cybersecurity services within ITU**

This section provides a comprehensive understanding of the fundamental cybersecurity elements implemented to safeguard the organization's digital assets.

2.1 **The prevention controls** encompass among other, tools and technologies that are used to support the cybersecurity framework, such as firewalls, intrusion detection systems, endpoint protection, and URL filtering. They are essential elements of ITU’s security architecture, providing a holistic layered and coordinated security approach to help ensure the confidentiality, integrity, and availability of sensitive information and critical systems.

2.2 ITU has a well-defined, organization-wide **Vulnerability management program** with a structured approach to identifying, evaluating, prioritizing, and mitigating potential security vulnerabilities in ITU's systems and applications. The program is designed to proactively identify vulnerabilities and reduce the risk of a cyber-attack by regularly assessing ITU's security posture. To improve collaboration between bureaus and different departments, vulnerability dashboards provide an overview of the current security posture vis a vis of their assigned digital assets.

2.3 **Access control and identity management** are key parts of ITU's security framework, preventing unauthorized access to information and resources, and reducing the risk of security incidents. ITU staff identities are centrally managed, but some external identities are managed locally. The organization has strengthened its password policy for delegates to mitigate the risk of account compromise and follow security best practices.

2.4 To promote a cybersecurity culture and strengthen the "Human Firewall," a mandatory IT security awareness and training program is now in place for all staff. The program is designed to educate staff on the importance of safeguarding information, data, and resources within the organization's IT infrastructure.

2.5 ITU's Security Operations Center (SOC) and Incident Response (IR) functions are vital for its cybersecurity framework, serving as the central components for detection and response controls. The SOC monitors and analyzes the security posture to identify and respond to potential threats. To provide around-the-clock monitoring and advanced cybersecurity expertise, ITU uses a hybrid SOC model, utilizing both managed security service providers (MSSPs) and in-house cybersecurity personnel.

2.6 To maintain a strong security posture, ITU is using continuous monitoring and threat landscape analysis to stay up to date on the latest threats and vulnerabilities and taking a proactive approach to security. ITU is also partnering with other UN entities such as the United Nations International Computing Center (UNICC) Common Secure, and the United Nations Chief Executives Board for Coordination (CEB), United Nations Information Security Special Interest Group (UNISSIG), to leverage its expertise and remain current on the latest threats and vulnerabilities.

2.7 ITU is conducting regular penetration testing against some of its mission-critical applications to proactively address security weaknesses and improve the overall security posture. The purpose of this service is to identify security vulnerabilities that could potentially be exploited by a real attacker, and to test the effectiveness of the ITU's security controls.

2.8 To ensure the security of the new working methods, like virtual meetings and teleworking, proactive measures have been implemented to mitigate cybersecurity risks. ITU has collaborated with the CEB and the UNISSIG working group to develop comprehensive recommendations for the use of virtual meetings.

2.9 ITU has developed an array of measurable and actionable security metrics to aid the organization in making informed decisions about the cybersecurity posture and prioritize its security efforts.

2.10 ITU has integrated the physical and cybersecurity divisions within the same department (ISD).

**3.** **Roadmap and further improvements**

3.1 As previously noted, the cyber threat landscape is rapidly evolving, and one of the latest challenges is the emergence of artificial intelligence (AI) as a transformative technology. ITU’s cybersecurity framework will need to leverage the use of AI-based security tools and solutions that can detect and respond to these threats not at human-speed but at machine-speed.

3.2 Harmonizing ICT services, particularly access control and identity management, can provide multiple benefits for ITU’s cybersecurity posture. It ensures consistency across different systems and applications, standardizing access control measures for better protection. Additionally, it can lead to cost savings by reducing the complexity and redundancy of access control systems.

3.3 While significant technological and operational measures have been implemented to prevent cyber-attacks, educating every staff member on their role in protecting the organization's information remains a persistent challenge. It is, therefore, imperative to empower staff to take an active role in improving organizational cyber resilience.

3.4 To enhance organizational cyber resilience, it is important to mainstream cybersecurity across the entire regulatory frameworks ([CWG-FHR-15/5](https://www.itu.int/md/S22-CWGFHR15-C-0005/en)), by integrating cybersecurity elements directly into the policies, processes, and practices of departments such as human resources, procurement, communications, or legal services.

3.5 Enhance cyber resiliency and recoverability through cyber drills, simulating various types of cyber-attacks, such as phishing or ransomware, in order to test the ability to respond effectively and efficiently to such incidents.

3.6 Departments and bureaus involved in software development activities can benefit from adopting a comprehensive best practice software development life cycle (SDLC). By doing so, they can ensure that security requirements are considered during the design phase and that the overall system architecture's business impact risk is analyzed thoroughly.

3.7 Given the increasing reliance on digital resources and adoption of new technologies and services within ITU, it is imperative to ensure a strong cybersecurity function in the ITU. With the expanding threat landscape and the need to maintain a robust security posture, having adequate cybersecurity function will enable ITU to proactively detect, prevent, and respond to potential cyber-attacks. While ITU has focused on technical cybersecurity measures, there's a need for improvement in non-technical areas such as user training, insider threat management, and data governance and classification. The goal, as stated in Council Doc 23/52, is to have appropriate security measures in place based on data classification and criticality, ensuring readiness to detect, respond to, and recover from security incidents.

3.8 At present, there is insufficient knowledge of the cybersecurity posture of ITU's regional and area offices. It is necessary to conduct a cybersecurity assessment to detect any potential weaknesses or vulnerabilities in the IT infrastructure, and to improve the overall effectiveness of the organization's cybersecurity program.

3.9 In closing and as stated in the JIU report, many UN organizations are facing major cybersecurity challenges due to legacy systems and shadow IT. Similarly, ITU is also dealing with persistent issues caused by outdated systems and shadow IT that have inherent vulnerabilities and risks. To address this, ITU has taken the auditors' advice and conducted a thorough assessment of its legacy systems.

**4. Financial implications**

Necessary improvements covered in section 4 above and their financial implications will be assessed in the course of the implementation of the Transformation Roadmap to Achieve Organizational Excellence (C23/52).

**5. Recommendations**

The CWG-FHR is invited to **consider the report and provide strategic guidance** on the implementation of the further improvements.

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

1. UN ORMS policy was approved by the UN CEB in 2014 and adopted by the ITU council in 2016 [↑](#footnote-ref-1)