|  |  |
| --- | --- |
|  | **Document CWG-FHR-17/5** |
| **20 December 2023** |
| **English only** |
|  |  |
| Contribution by the secretariat | |
| REPORT ON ESTABLISHING A GOVERNANCE STRUCTURE FOR CYBER SECURITY, IT AND DATA/INFORMATION | |
| **Purpose**  This document proposes a comprehensive governance framework, responding to the IMAC recommendations regarding the need for a resilient governance structure for IT, Cybersecurity and data, leveraging existing committees like the ICTC, with representatives from the general secretariat and three bureaus. This proposed structure distinctly separates governance and operations for IT, cybersecurity, and data. Governance sets strategic goals, direction, and policies, while operations implement and execute activities to achieve these goals.  **Action required**  The CWG-FHR is invited **to note** the report.  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  **References**  *Council documents* [*C23/22*](https://www.itu.int/md/S23-CL-C-0022/en)*,* [*C23/52*](https://www.itu.int/md/S23-CL-C-0052/en)*,* [*C23/INF/11*](https://www.itu.int/md/S23-CL-INF-0011/en)*,* [*C22/57*](https://www.itu.int/md/S22-CL-C-0057/en)  [*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* | |

1. **Background**

This document addresses recommendations from [CWG-FHR-16/6](https://www.itu.int/md/S23-CWGFHR16-C-0006/en), and those of the Independent Management Advisory Committee's (IMAC) that call for a robust cybersecurity governance structure. IMAC emphasizes the need for a comprehensive framework covering technical and strategic aspects, ensuring decision-making authority, demand management, accountability, and performance incentives.

Additionally, IMAC recommends a top-down data governance framework with retention policies to safeguard historical data, aligning with [C23/22](https://www.itu.int/md/S23-CL-C-0022/en) and [C22/57](https://www.itu.int/md/S22-CL-C-0057/en) principles. Document [C23/INF/11](https://www.itu.int/md/S23-CL-INF-0011/en) highlights technical risks due to the absence of a digital/IT strategy and governance structure, leading to unclear ownership and direction.

In response, this document proposes an overarching governance framework leveraging existing committees, notably the ICTC, encompassing IT, cybersecurity, and data. The proposed structure explicitly separates governance and operations for these services, with distinct roles and purposes.

The committee would report to the Secretary-General/Deputy Secretary General and receive inputs from the recommendations from the Compliance Dashboard, encompassing internal and external oversight bodies like the newly created oversight unit, IMAC, external auditors, Joint Inspection Unit, Chief Executives Board and finally subject matter experts.

# 2. Cyber security governance

The Cybersecurity Governance Committee oversees end-to-end business and IT responsibilities for cybersecurity, aligning with organizational strategic goals. Key functions include:

1. **Strategy Development:** Establishes the strategic direction for cybersecurity initiatives, aligning with business objectives, identifying critical assets, and guiding resource allocation.
2. **Policy Formulation:** Develops and updates cybersecurity policies, ensuring adherence to best practices, legal requirements, and organizational objectives.
3. **Risk Management:** Oversees cybersecurity risk management, maintaining an acceptable risk level, setting tolerance thresholds, and conducting regular risk assessments and audits.
4. **Compliance and Regulatory Oversight:** Ensures adherence to regulations and internal policies, providing advice on oversight recommendations.
5. **Incident Response and Crisis Management:** Supervises the organization's response to incidents, developing and maintaining a comprehensive incident response plan.
6. **Performance Monitoring:** Establishes KPIs and metrics to measure the effectiveness of the cybersecurity governance framework, providing regular reports to executives.
7. **Stakeholder Engagement:** Fosters collaboration among IT, legal, compliance, risk management, bureaus, and business units, ensuring alignment with cybersecurity objectives.
8. **Business Continuity:** Ensures the organization's resilience against cybersecurity incidents, maintaining continuous services and implementing business continuity measures for timely recovery.
9. **Fields Offices**: Address security concerns and the review of risk mitigations related to the field offices and ensure consistent enforcement of cybersecurity across the organization and at ITU events.

# 3. IT governance

In addition to cybersecurity governance, the Committee oversees IT governance, focusing on strategic alignment, resource optimization, and risk management. Key activities include:

1. **IT Strategy Development:** Defines the organization's IT strategy, aligning with overall goals and supporting digital transformation and innovation initiatives.
2. **Resource Oversight:** Ensures optimal allocation of IT resources, including budget, personnel, and infrastructure.
3. **Service Performance:** Ensures reliable, responsive, and cost-effective IT services meeting internal and external stakeholder needs.
4. **IT Risk Management:** Collaborates with the risk management team to oversee IT risk mitigation within the organization's risk appetite, integrating it into the overall risk management framework.
5. **Compliance Oversight:** Ensures IT policies, processes, and systems comply with ITU service orders, regulations, and contractual requirements.
6. **Project and Portfolio Oversight:** Manages IT projects and portfolios, ensuring alignment with strategic objectives, resource adequacy, budget adherence, and successful outcomes.
7. **Innovation and Emerging Technologies:** Fosters an innovative culture, encouraging exploration and adoption of emerging technologies for resilience, process improvement, enhanced customer experiences, and competitive advantage.
8. **Governance Integration:** Promotes the integration of IT, cybersecurity and data governance, ensuring a holistic approach to managing technology risks.
9. **Auditing and Accountability:** Establishes a robust IT audit and accountability framework for effective, efficient, and compliant IT processes and systems.

# 4. Data/information Governance

In addition to its roles in IT and cybersecurity governance, the committee will also manage the oversight of data/information governance. As part of this responsibility, the committee is actively engaged in ITU's comprehensive information governance program for Microsoft 365. The program is designed to foster organization-wide information management practices, behaviors, and processes, with a focus on unlocking the value of our information assets.

Key tasks within this initiative include:

1. **Data Security:** Preventing accidental sharing of sensitive information to ensure robust data protection.
2. **Data Classification:** Implementing a system for categorizing data to enhance its understanding, accessibility, and security.
3. **External Access Management:** Safeguarding data through controlled access, particularly when shared externally.
4. **Provisioning of Data Storage Collections:** Ensuring secure data storage with well-defined security measures, metadata, and governance controls.
5. **Information Discovery:** Facilitating the efficient discovery of information within the organization.
6. **Lifecycle Management:** Implementing strategies to manage the entire lifecycle of information effectively.

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