



UNITED NATIONS SYSTEM

Chief Executives Board for Coordination

CEB

CEB/2022/HLCM/DTN/10

12 June, 2023

**Digital & Technology Network Session Report**

International Monetary Fund (IMF) Headquarters, Washington D.C.

1 – 3 May, 2023

**Contents**

Executive Summary.....	3
Background .....	4
Opening of the Meeting.....	4
Opening Remarks .....	4
Emerging Technology Trends.....	4
CIO Priorities .....	5
Microsoft Solutions.....	5
Intelligent Data Platform.....	5
Copilot 365 .....	6
Open Source Software .....	7
UN Maps .....	7
Quantum .....	8
DTN Working Groups .....	9
Digital Transformation .....	9
Digital Accessibility.....	9
ERP .....	9
CRM .....	10
Cloud .....	10
Open-Source Software.....	11
Mutual Recognition.....	11
Collaboration Technologies .....	11
Migrating Towards Communities of Practice.....	11
Outcomes .....	12

Cybersecurity .....	13
Zero Trust .....	13
Ransomware .....	13
Information Security at Meetings .....	14
Cybersecurity In Emergencies .....	14
Cybersecurity Baseline .....	15
Outcomes .....	15
Digital Advice to Member Countries .....	16
Global Digital Compact .....	16
UN 2.0 .....	17
Balancing AI Risks and Opportunities .....	17
Outcomes .....	19
NASA’s Digital Transformation Journey .....	19
Digital Transformation in the UK Government .....	20
The Role of Chief Digital Officer .....	21
Common Denominators .....	22
Breakout Sessions .....	23
Conclusions .....	24
Communities of Practice .....	24
Future Meeting Format .....	25
Autumn Session Date and Venue .....	25
Autumn Session Agenda .....	25
Subsequent Sessions .....	25
Virtual Session on AI .....	25
Annex 1 – Agenda .....	27
Annex 2 –Participants .....	35
Annex 3 – DTN Minimum Baseline for Cybersecurity .....	38
Version 3 - 2023 .....	38
Cybersecurity Baseline Appendix – Alignment with Industry Standards and Best Practices .....	42

## Executive Summary

*The meeting sparked vibrant discussions across multiple domains, with a significant focus on the transformative power of digital technologies. Digital transformation emerged as a central theme, emphasizing the need for a strategic and holistic approach that goes beyond IT. The imperative of aligning digital transformation efforts with the common good was underscored, emphasizing the importance of ongoing dialogue between business, IT and other stakeholders. Participants recognized the need to minimize duplication, identify synergies, and drive common themes throughout the UN system. By harnessing the potential of digital transformation, UN aims to unlock new opportunities, enhance efficiency, and drive positive impact across its diverse domains. Decisions made reflected the interest these topics generated and resulted in the establishment of a new communities of practice.*

Topics discussed included cybersecurity and Zero Trust, generative AI, open source, data strategy, digital accessibility, CRM & ERP, emerging solutions in many of these domains and how to effectively facilitate the sharing knowledge within a growing community. Cybersecurity discussions focused on adopting an incremental approach and implementing Zero Trust principles for enhanced security. The role of generative AI in shaping society and work was discussed at length and alignment with the common good was highlighted as an underlying objective. The value of open source in promoting contributions and scalable architectures was recognized and advanced by the introduction of a dedicated community of practice. Updates on the UN data strategy and data analytics developments benefited from recent improvements in data collection and sharing platforms, providing for advanced insights. The importance of sharing scalable solutions and fostering collaboration for mutual benefit was also emphasized, reflecting the meeting's focus on progress and advancement within UN.

Moving forward, this meeting laid the foundation for crucial next steps across many domains, reflecting widespread interest. In the realm of cybersecurity, the Network has adopted an incremental approach towards implementing Zero Trust principles, while also approving version three of the cybersecurity baseline. Discussions on Artificial Intelligence (AI) were informed by pre-meeting surveys and recognized the significance of timely deliberations on the topic and to help actors on the global stage steer advances towards the common good. The Network has committed to further exploring this matter in a dedicated session in the upcoming weeks, with the aim of formulating a common position and recommendations for the attention of higher management. A Digital Accessibility Working Group was established to propose guidance in the area of ICT, which may also be applied towards the introduction of a common baseline. Deliberation on the topic of open-source software translated to the formation of a new community of practice and the commitment to contribute to the broader open-source community through the adoption of scalable architectures. A collective commitment was made to improve data collection, sharing and exchange with the introduction of cross-references to UN 2.0 in member organizations' own ICT strategies. The importance of mutual recognition to expedite the dissemination of scalable solutions was duly acknowledged, particularly with regard to the provision of "business as a service" and discussion on this topic resulted in a new working group.

It was concluded that addressing these matters effectively will be aided by a formal digital transformation community of practice, to be established based on meeting participation. This new community will focus on topics directly relevant to the participants and build upon the key outcomes of this meeting. Furthermore, annual meetings will be organized as a platform to foster collaboration and facilitate knowledge exchange between the two communities and other stakeholders.

## Background

Invitations to this session were sent to Chief Digital Officers (or equivalent representatives) from CEB member organizations. The approach centered around fostering an inclusive environment, encouraging the sharing of information (as well as contact details), to facilitate productive discussions among colleagues working in domains that have become increasingly intertwined. Consequently, participants consist of a diverse group of professionals with expertise in various areas of technology and innovation, including strategic IT management, data science, digital transformation, and emerging technologies. Discussions provided the opportunity to share valuable insights and experiences related to information management, ICT services, digital advisory services, and driving innovation within the organization.

## Opening of the Meeting

The 2023 spring session of the Digital & Technology Network (DTN) was kindly hosted by the International Monetary Fund (IMF) at their headquarters in Washington D.C., between 1 and 3 May. The meeting convened 66 participants from 48 entities, including Chief Information Officers (CIOs) and Chief Digital Officers (CDOs). The agenda included 26 presentations covering 32 items, updates from 6 DTN working groups and concluded with breakout sessions exploring future courses of action. New members were welcomed from ICAO & UNAIDS. The meeting was chaired by Bernardo Mariano Junior (CITO, UN) and Shirin Hamid (CIO, IMF). The agenda was adopted without changes.

## Opening Remarks

Mr. Bo Li (Deputy Managing Director, IMF) welcomed the participants by underlining the crucial role of technology in global economic growth and transformation and the need to leverage advancements while managing risks. Collaboration was encouraged to build a safer, more inclusive digital economy. Mr. Li expressed optimism that the event's conclusions and recommendations would offer innovative strategies to enhance economic and financial stability, cybersecurity, and sustainable growth.

## Emerging Technology Trends

Marty Resnick (Gartner) presented three strategic trends identified by Gartner. Marty explained that CIOs need to determine their role and accountability in analyzing these trends and their impact. They also need to manage stakeholders while ensuring internal capacity and organizational model can respond to these trends effectively.

The importance of considering factors beyond technology, such as trust, security, ethics, and privacy was emphasized during the presentation. Mr. Resnick introduced the concept of AI TRiSM, which focuses on optimizing trust in AI and managing risks associated with AI models. He provided case studies and examples of organizations integrating ethics, privacy, and security into AI development. There was a discussion on generative AI and its potential impact on job augmentation or replacement. Mr. Resnick mentioned the growth of generative AI models for code generation and synthetic data generation and encouraged considering the opportunities, risks, accelerators, and inhibitors of generative AI through an impact mapping exercise. He emphasized the importance of examining trends from various perspectives, including technology, politics, economics, social trust, regulatory, and environmental concerns.

The discussion covered several topics including AI trends, explainability, governance, and the link between mini apps and citizen development. It aimed to explore the opportunities and challenges associated with AI in the context of current technological advancements. Key points discussed included the use of synthetic data and its projected implementation, the importance of making AI models explainable with examples of mathematical explainability and human testing, the connection between mini apps and

citizen development through super apps and low code/no code platforms, the need for governance practices in AI adoption and the creation of learning management systems, the balance between revealing AI's inner workings and the associated risks of hacking, and the importance of considering the broader implications of technologies like quantum computing. There was an emphasis on the need for ongoing research and staying informed to effectively navigate the evolving landscape of AI.

## CIO Priorities

Brian Jackson (Info-Tech) provided insights from a CIO perspective on how to respond to these trends and develop the necessary capabilities and operating model. The CIO's priorities for tackling these challenges include adjusting IT operations to manage for inflation, preparing the data pipeline for AI training, adopting zero trust security, engaging employees in the digital age, and shaping the IT organization to improve customer experience. These priorities require considerations of budget increases, data quality and governance, AI adoption risks and opportunities, and the implementation of zero trust architecture for enhanced cybersecurity. The examples of other CIOs navigating these priorities highlight the importance of vendor negotiations, financial oversight of cloud operations, data-driven insights, and the adoption of zero trust model for security. Taking action on these priorities involves adjusting IT operations to account for inflation, improving data quality, leveraging AI capabilities, and adopting zero trust security measures.

During the discussion, participants explored several key areas of focus and challenges faced by IT leaders. The conversation centered around the significance of organizational change management during technology initiatives. Participants stressed the need to identify different user groups within the organization to tailor communication and support effectively. Cloud management emerged as a major concern, with a particular focus on cost management. Participants highlighted the importance of dedicated teams and strategies to optimize cloud expenses and suggested renegotiating terms and leveraging contracts. Another point of discussion was the realization of benefits from various programs and projects. Participants emphasized the need to drive value and benefits, especially in areas such as generative AI and emerging technologies. The shift to a hybrid workforce sparked conversations about its effectiveness and associated recruitment challenges. Attracting talent and addressing expectations for remote work were identified as hurdles. Additionally, the changing perception of IT departments from support functions to strategic business drivers was explored. While progress was observed in the private sector, the public sector was perceived as lagging behind in this regard. Aligning IT priorities with organizational initiatives was emphasized, with participants suggesting scenario planning exercises and customization based on specific goals. Lastly, there was recognition of the existing gap between the current state and desired future state of IT departments, prompting the need for strategies and roadmaps to bridge this disparity. Overall, the discussion shed light on the challenges and focus areas for CIOs, stressing the importance of alignment, effective change management, cost optimization, benefits realization, talent acquisition, and IT department transformation.

## Microsoft Solutions

### Intelligent Data Platform

Marc Reguera (Microsoft) and Patrick LeBlanc (Microsoft) presented Power BI and Synapse product groups, highlighting current and upcoming capabilities, including the evolution from predictive to prescriptive analytics. In addition, results of a DTN survey (No-Code, Low-Code at Workplace) were shared with members in advance of the meeting.

The focus of the discussion was on Microsoft's advancements in various products and services, particularly in the Azure platform and Office 365 space. The agenda included a preview of upcoming releases related to the integration of Power BI and data analytics tools, as well as their connection to copilot and generative AI. The presentation emphasized the benefits of these new capabilities in terms of data analytics and how they can be leveraged within organizations. The speaker highlighted the challenges of data integration and the need for a unified solution, introducing Project Trident as a comprehensive product that brings together various Microsoft services into a single platform. The presentation discussed features like a shared user experience, optimized AI capabilities, and a unified security model. The concept of a "one leg" storage system was introduced, offering a unified storage solution for all users and enabling collaboration among different roles and personas. The use of the Delta and Parquet format was emphasized as a standardized, open format for data storage and transformation. The presentation concluded with a demonstration showcasing the benefits of the proposed approach, including improved performance and seamless data access.

The discussion revolved around the power and limitations of AI and its role as a programming language. The participants acknowledged the potential of AI as an assistant but also emphasized the need for responsible use and human oversight. They discussed the importance of understanding the limitations of AI models and the ability to provide feedback for improvement. The participants mentioned the need for customization and integration in big data projects and raised questions about optimizing code, language translation, and productivity gains. Data sovereignty, governance, and security were also important considerations, with a focus on striking a balance between self-service and centralized control. The participants highlighted the need for further discussions with the account team to address specific concerns and ensure secure and governed solutions.

#### Copilot 365

Steve Gemmel (Microsoft) and Steven Lough (Microsoft) introduced the topic of AI and its potential to transform the world. Speakers highlighted the maturing technology of large language models like ChatGPT and the effectiveness of chat interfaces in enabling communication with AI systems and the challenge of dealing with unstructured data and the need for efficient solutions to extract valuable insights. Results of DTN survey (ChatGPT at Workplace) were shared with members in advance of the meeting.

Microsoft's proceeded to present Copilot, an AI-powered tool integrated into various products, including M365 applications, which aims to enhance productivity and provide instant answers and assistance. Examples were given, such as generating documents in Word and creating presentations in PowerPoint with the help of Copilot. They stressed the importance of leveraging AI to improve efficiency and productivity without additional resources, and the potential impact on the 2030 agenda and post-COVID recovery efforts. The session showcased the capabilities of Copilot and its integration with different Microsoft platforms to address various business needs.

The discussion that followed primarily revolved around upcoming releases, including the intelligent data platform and Microsoft 365 copilot. The release date of the intelligent data platform raised considerations for transitioning ongoing data programs, while the release of Microsoft 365 copilot was postponed, allowing organizations more time to address integration challenges. The extensive integration of Microsoft 365 suite of products was emphasized, highlighting its presence in various applications such as PowerPoint, Word, email, and Teams. Participants were encouraged to formulate game plans to address the implications of generative AI and intelligent data within their organizations. The existence of an API working group in HLCP, which had established AI principles, was highlighted. A designated individual was

assigned to present these principles in a forthcoming session. Participants were invited to reflect and provide input on the implications of generative AI and Microsoft 365 copilot. The importance of governance in low code/no code platforms was discussed, with only a portion of participants having established governance measures.

## Open Source Software

The DTN held a panel Discussion, moderated by Herve Tourpe (IMF, Digital Advisory Unit Chief) on the topic of open source and developing countries (best practices). This panel brought together Ben Cervený (Foundation for Public Code); Lorena Cano, (IADB) and Devesh Sharma (Gates Foundation) to examine the role of international organizations in promoting this transition and share their insights on the latest trends in government adoption of open source, access, data and knowledge.

During the discussion, the importance of open-source solutions and the benefits of reusing and updating tools with strong documentation was emphasized. The panel highlighted the role of community contributions in implementing open-source digital tools, focusing on capacity building and workshops to educate developers. They invited participants to join the code for Development Network and access showcases with over 2,000 developers. The concept of stewardship in the public sector was discussed and lessons learnt from working with various applications and municipalities were shared. Panelists emphasized the need for adaptiveness and sustainability in software development and the importance of open standards and reuse. Challenges in integrating systems were also seen to demonstrate the benefits of using open published standards and avoiding reinventing the wheel. They also highlighted the importance of building reusable and adaptable systems that can work with emerging technologies. The conversation touched on the need for collaboration and finding commonalities in large-scale projects, as well as the value of open source in facilitating decomposition and recombination of elements.

The question of where to begin when facing development challenges in projects was addressed in the ensuing discussion. Discussions highlighted the importance of identifying objectives and challenges to determine the best starting point and considered the availability of sustainable funding to keep maintain teams active for longer periods.

## UN Maps

Kyoung-Soo Eom (OICT), Diego Gonzalez Ferreiro (UNGSC) Alexandre Caldas (UNEP) presented UN Maps. The presentation discussed the challenges faced by UN in terms of insufficient geospatial data, mapping limitations, geopolitical sensitivities, and the need for accurate boundaries and geographical names. To address these challenges, UN introduced UN Maps, a package of geospatial services tailored to support their mandates and operations. UN Maps offers various products such as street maps, image maps, 3D globes, and operational maps, which provide detailed information for different purposes. The presentation highlighted the role of UN Maps as a foundational system and an enabler for technology and innovation across UN. It emphasized the collaboration with different entities, including Member States, OpenStreetMap, and UNGSC, to gather and validate topographic and base data. The workflow involves storing the data in a global repository and utilizing proprietary and open-source software for hosting and exposing the information. The presentation also mentioned the impact of UN Maps on fulfilling UN mandates and improving operational decision-making, verification processes, and environmental management. Additionally, it discussed the vision of integrating UN Maps into the one UN situation room, which aims to empower the use of geospatial information management and deliver on the Sustainable Development Goals. The presentation concluded by outlining the plans for a soft launch of the one UN

situation room and the selection of priority data teams to demonstrate the value of geospatial capabilities across the UN.

The discussion focused on GIS and its role in the ICT organization. Colleagues were asked about GIS integration and its importance. Topics discussed included data analytics, citizen development, and ICT and DTN's role in driving transformation. Concerns were raised about border disputes and how to address them. Presenters explained the importance of coordination and consistency and mentioned UN's standardized map. They clarified that the map doesn't endorse specific borders and used disclaimers to prevent misunderstandings. The presentation also considered technology strategy and GIS implementation, emphasized the need for scalability and avoiding duplication. They suggested DTN's involvement in efficient scaling and leveraging existing solutions. Access rights and data security were brought up as issues, both internally and for UN Maps. The need for proper access control and safeguards was acknowledged. Participants stressed the significance of governance in managing GIS effectively. They discussed clear governance structures, collaboration, and open GIS standards. DTN's role in governance and standardization was emphasized. Overall, the discussion highlighted coordination, scalability, governance, and leveraging existing solutions in GIS within UN. The goal was to maximize value, reduce duplication, and provide reliable geospatial information to member states.

## Quantum

Sylvain St. Pierre (UNDP) shared UNDP's journey of implementing the Quantum ERP system and the positive impact it has had on their organization. The primary goal of the project was to replace the outdated Atlas and streamline operational processes. Mr. St. Pierre discussed the timeline, challenges faced, and key learnings during the implementation process. They emphasized the importance of senior leadership commitment, teamwork, effective communication, data quality, testing, training, and post-implementation support for a successful deployment. The Quantum system was highlighted for its cloud-based architecture, integration capabilities, multilingual support, and potential for collaboration with partner agencies. The presentation concluded with insights on costs, scalability, and the overall significance of Quantum in driving operational effectiveness and achieving organizational goals.

The discussion focused on the challenges and opportunities related to ERP implementation and interagency collaboration. Participants acknowledged the complexity of implementing ERP systems across multiple agencies and commended UNDP for successfully implementing a fully RP system in a short time frame. The potential for code sharing and knowledge exchange, particularly in HR processes, was highlighted. Participants expressed interest in exploring partnerships with Organization3 and discussed long-term sustainability and cost considerations, including potential price increases. The concept of mutual recognition between ERP solutions was discussed, along with the idea of establishing a common back office for agencies operating in different locations. The debate between best-of-breed solutions and integrated suites was also addressed. Participants shared experiences with the selection process and emphasized the importance of compliance and contractual terms. The discussion provided valuable insights, emphasizing collaboration, solid business cases, and transparent procurement processes. Recommendations include further exploration of code sharing, engagement with UNDP, evaluation of sustainability and costs, consideration of a common back office, and ongoing collaboration among auditors, procurement officers, and legal teams.



## DTN Working Groups

The following updates are provided by existing DTN working groups, as well as those established during the session.

### Digital Transformation

During the meeting, Dino Cataldo Dell’Accio (UNJSPF) shared an update from the DTN Digital Transformation Working Group<sup>1</sup>. He discussed the work done since the last session in October and the representation of various entities in the organization. The focus was on assimilating input from external sources and defining digital transformation for the organization. Mr. Dell’Accio proposed a definition that involves using digital technology to make fundamental changes in processes, culture, and user experiences, ensuring continuous improvement and being fit for purpose. The discussion also involved tools for measuring digital transformation, common elements found in different examples, and recommendations for collaboration, innovation, and governance. The meeting concluded with plans to further discuss the presented ideas and prioritize areas for action.

### Digital Accessibility

Suzanne Shanahan (UN), Edmund Tam (ITU) and Celine Hazbun (WHO) presented High Level Review of ToR & Deliverables for the proposed working group on Digital Accessibility. The presentation focused on the importance of digital accessibility and the proposed establishment of a digital accessibility working group within the organization. The presenters emphasized the need to consider digital accessibility as a core component of solution development to ensure that individuals with disabilities can effectively use digital systems. The presentation highlighted the goals, objectives, and proposed terms of reference for the working group. Data collected through a DTN survey on digital accessibility was shared, highlighting areas where organizations are at different levels of maturity. An overview of the organization's accessibility policy and initiatives to promote digital accessibility was shared and supplemented with insights into the organization's digital accessibility strategy, which notably includes cultural shifts, governance, processes, and tools. The presentation underscored the importance of collaboration, training, and continuous improvement to achieve digital accessibility goals.

The presentation concluded by emphasizing the significant impact of digital accessibility on the lives of individuals with disabilities and the need for organizations to prioritize accessibility as an integral part of their digital initiatives.

### ERP

Marthinus Johannes Greyling (UNHCR) provided an update from ERPSIG<sup>2</sup>. Marthinus summarized the results of an ERP survey carried out between February and March 2023. The main objective of the survey was to gather data on the current application landscape of 15 organizations. While feedback was appreciated, there were a few organizations that required clarification regarding the data provided. The collected data will be utilized in an analysis conducted by Deloitte, based on the terms of reference provided. The study will focus on potential savings, collaboration opportunities, and future application landscapes. The findings of the study will be shared with the committee and the participating

---

<sup>1</sup> Members of the current Digital Transformation Working Group include: UNJSPF\*, UNOPS, ITU, FAO, UNEP, CTBTO, IAEA & UNIDO. Membership of this group is to be expanded and WG will become a community of practice.

<sup>2</sup> Membership of ERPSIG currently includes: CTBTO, ECOWAS Commission, ESA, FAO, IAEA, IARC, ICC-CPI, ILO, IMO, ITC-ILO, IOM, ITU, OECD, UN Secretariat/ERPSD (Umoja), UN Secretariat/OICT, UNESCO, UNHCR\*, UNICC, UNICEF, UNIDO, UNJSPF, UNRWA, UNWTO & WFP\*.

organizations in a forthcoming update. Additionally, future meetings will feature presentations from organizations discussing noteworthy developments. The survey addressed aspects such as upgrade plans, implementation timeframes, cloud adoption, and the future of applications. The report concludes by encouraging organizations not included in the initial survey to reach out to UNHCR or WFP to participate and provide valuable feedback.

#### CRM

Dino Cataldo Dell'Accio (UNJSPF) provided an update from the CRM Working Group<sup>3</sup>. Mr. Dell'Accio discussed the implementation of an account and contact management system within their organization. They highlighted the core importance of this implementation and the integration of various functionalities, including financial models, logistic integration, access control, and CRM capabilities. They emphasized the significance of change management, both internally and externally, and aligning the project with the strategic plan while measuring its impact through defined key performance indicators. Rationalizing language scales, eliminating silos, and considering reporting capabilities were also addressed. The presentation stressed the need for continuous improvement and adaptation to evolving technology.

The creation of a CRM special interest group to explore opportunities for improvement and synergies was put forward, with the possibility of co-locating meetings with the ERPSIG. The goal is to drive collaboration and share lessons among front runners and organizations at different stages of implementation. This approach, which also recognized the need for representation and support for all organizations, was adopted.

#### Cloud

Erzen Ilijazi (UN) provided an update from the Cloud Working Group<sup>4</sup> focused on FinOps. Mr. Ilijazi explained that the Cloud FinOps working group is investigating cloud procurement and brokerage, cost control, cost recovery, cost forecast and consists of 9 Members from 8 organizations. It is tasked with developing a FinOps framework suitable for UN Organizations and propose roadmap for its implementation. Work Completed includes identifying the main challenges in establishment of FinOps in the UN Organizations; Identified personas, KPIs and main tools to measure and control cloud expenditure and adopting the FinOps Foundation framework. Final Deliverables will include a White paper on FinOps (In progress); Roadmap agreed with all members and best practices and standards for implementation of FinOps. Next steps include the establishment of a road map to implement FinOps in UN Organizations and the identification of best practices and common framework for clients and providers entities in UN.

Francesca Duri (WIPO) provided an update from the Cloud working group investigating a UN Private Cloud opportunity, defined as a private environment for utilization by all entities. Ms. Duri explained that this group has seen particularly active participation and productive discussions from 10 participating agencies. They emphasized the significance of a private cloud and its feedback process. An internal survey was conducted to gather input for future steps. The focus is on determining the type of services the private cloud should offer and considering factors like managed or self-service options. The discussions highlighted the need for criteria to guide workload decisions between public and private cloud. Lastly, a feasibility study was mentioned as part of the plan.

---

<sup>3</sup> Members of the CRM Working Group include: UNJSPF\*, UNOPS, ITU, UN Secretariat, FAO, UNCTAD, UNDP, GC-FUND, OPCW, UNICEF & UNEP.

<sup>4</sup> Membership of the Cloud WG includes: FAO, IAEA, ICC-CPI, IFAD, IOM, ITU, UNAIDS, UNDP, UNFPA, UNGSC, UN Secretariat\*, UNICC, UNICEF, UNIDO, UNOG, UNOPS, UNU, UNWRA, UPU, WFP, WHO, WIPO\* & WTO.

### Open-Source Software

Omar Mohsine (UN) put forward proposal to create a community of open-source specialists and leverage existing partnerships and promote the adoption of open-source solutions, both operationally and in programmes. Soren Thomassen (UNFPA) offered to Co-Chair this community.

In his presentation, Omar referenced the vast number of applications developed within the UN system was acknowledged, emphasizing open source as a language that connects global communities. The focus was on sharing and institutionalizing open-source solutions, highlighting the need for standardization and empowering OSS teams with best practices. Membership in the Digital Public Good Alliance was mentioned, expressing interest in expanding towards digital public goods. The proposal to establish a working group was presented, accompanied by shared Terms of Reference.

Participants recognized the need to address bottlenecks and set clear priorities in order to facilitate mutual recognition. They emphasized the significance of interoperability, shared services, and quality control when exploring use cases that tap into the open-source marketplace. The upcoming sub working group meeting was highlighted as an opportunity for teams to address questions and comments.

### Mutual Recognition

Tata Velayo (UN) put forward the concept paper shared with HLCM at its recent session on Mutual Recognition and the establishment of a Working Group<sup>5</sup>. The concept note (approved by HLCM in April 2023) describes the mechanism operating as a sub-working group (under the umbrella of the HLCM Coordination Group on MR). HLCM-expected deliverables to advance MR in ICT include the establishment of a mechanism for UN entities to share and compare policies, practices and systems; the development of a framework of policy instructions and guidelines for MR in ICT among collaborating entities to bridge the gap in differences in policies practices and systems. An update is to be provided to DTN at its autumn session.

### Collaboration Technologies

After having concluded its initial two-year term, OPCW was renominated as Chair the Collaboration Technologies Working Group.

### Migrating Towards Communities of Practice

Discussions also considered the nature and naming conventions applied to DTN working groups and specifically to review and consider their renaming to communities of practice.

Working Groups (WGs) are defined as formed for a specific task or project and is disbanded once its objectives are achieved, while a community of practice as a more sustained community focused on ongoing learning, collaboration, and knowledge sharing within a particular domain. Special interest groups (SIGs) focus on addressing specific issues or advancing knowledge in a specialized area, whereas a community of practice (CoPs) emphasizes ongoing collaboration, learning, and knowledge sharing within a specific professional domain. The distinction between the latter two is blurred. But while WGs and SIGs tend to have a more targeted and issue-specific focus, CoPs are known for their broader scope, fostering long-term engagement and relationship-building among participants. In support of harmonization, CoP is therefore the proposed term to be applied where the distinction applies.

---

<sup>5</sup> Membership of the DTN Mutual Recognition WG currently includes UN Secretariat\*, UNDP, UNJSPF, UNFPA, WMO, UNICC & UNESCO.

The following list includes existing and proposed groups, for an evaluation to be made and excludes their respective sub-groups:

*Current DTN Working Groups:*

- Cloud Adoption Working Group (renaming to 'Cloud' recommended)
- Digital Transformation Working Group
- Customer Relationship Management (CRM) Working Group
- Collaboration Technologies Working Group

*Current DTN Special Interest Groups:*

- UN Information Security Special Interest Groups (UNISSIG)
- ERP Special Interest Group (ERPSIG)

*Working Groups established during session:*

- Digital Accessibility Working Group
- Open-Source Software Working Group
- Mutual Recognition Working Group

*Working Groups sunset during session:*

- Enterprise Architecture Working Group (activities subsumed by Cloud WG)

*New Community of Practice proposed at session:*

- Digital Transformation Community of Practice

Outcomes

- DTN to evaluate naming conventions applied to existing and proposed Working Groups/Special Interest Groups.
- DTN took note of progress reported by the Digital Transformation WG. A CoP on Digital Transformation is to be established, to include CDOs and equivalent roles. A proposal is also to be submitted by the CoP for review on the definition of Digital Transformation within the UN system. Annual DTN meetings to convene both (CIO & CDO) communities for partial session. Separate interim CDO sessions to be planned in parallel.
- DTN accepted the Terms of Reference for the DTN Digital Accessibility WG, including the development of proposed guidance and a common baseline. Kick-off meeting to be announced and scheduled in the short-term.
- UN/UNFPA to lead a community of open-source software specialists and leverage existing partnerships and promote the adoption of open-source solutions, both operationally and in programmes. ToR of WG was approved during session and kick-off meeting to be scheduled.
- DTN took note of progress made by CRM WG and asked it to establish a CRM community and plan parallel and co-located periodic meetings with ERPSIG. The newly established CRM WG will provide input to the upcoming virtual ERPSIG. Discussion within this WG to focus on the outcome in the context of ERP next generation platforms.
- United Nations Cloud WG to present at the next DTN session:
  - Guidelines on best practices and standards for the implementation of FinOps in the United Nations, including roadmap for its implementation
  - Common definition of the UN private cloud, baseline services for the Minimum Viable Product (MVP) and the map of the UN datacenters that can be used for a private cloud hosting

- Concept paper on Mutual Recognition in ICT approved. OICT will schedule a meeting with DTN Sub working group on MR in Q3 to discuss possible initiatives.
- The group on Architecture was officially sunset on the basis of no activity and scope subsumed by Cloud working group.

## Cybersecurity

### Zero Trust

John Kindervag, Founder of Zero Trust presented concept of Zero Trust, emphasizing its significance in preventing data breaches and enhancing cybersecurity resilience.

The presentation emphasized the need to approach Zero Trust implementation iteratively, focusing on individual protect surfaces and gradually improving them. The Kipling method, a policy construct used in Zero Trust, was introduced, emphasizing the importance of defining access based on the principles of who, what, where, why, and how. The presentation also touched upon the use of appropriate tools and technology to implement Zero Trust effectively, the significance of understanding and protecting crown jewels or critical assets, and the challenges and solutions related to software as a service (SaaS) adoption within a Zero Trust framework. Overall, the presentation provided insights and guidance for organizations embarking on their Zero Trust journey.

Discussion addressed misconceptions surrounding Zero Trust, such as the notion that it involves making a system trusted. The importance of eliminating the idea of trust in digital systems was emphasized, as trust can be both a vulnerability and an exploit. As an initial step towards increased security in cloud environments, organizations were recommended to segment (cloud-based) application environments, implement Layer 7 application aware controls as a starter for segmenting cloud service security.

Hans de Jong (IAEA) and Sachiko Hasumi (IOM) presented an update on behalf of the UN Information Security Special Interest Group (UNISSIG),<sup>6</sup> addressing the outcomes and ongoing work of working groups and the revised cybersecurity baseline.

### Ransomware

It was recognized in recent sessions of HLCM, FBN and UNISSIG that addressing data protection, data privacy risks, ransomware response, and cyber risks requires a cross-functional approach. Likewise, the Risk Management forum (RMF) emphasized the importance of learning from each other. As a result, the RMF established a working group to provide guidance and develop a common approach to the issue of ransomware. One track, led by UNISSIG Co-Chair Sachiko Hasumi (IOM) provided an update on progress made by this Working Group<sup>7</sup> towards the establishment of common SOPs, and a white paper supporting recommendations in preparation for HLCM's fall session. This whitepaper presented a compendium of ransomware resources and procedures that exist in UN organizations. Conclusions of this working group,

---

<sup>6</sup>

Membership of UNISSIG (including observer organizations) currently includes: UN, FAO, IAEA\*, ICAO, IFAD, ILO, IMF, IMO, IOM\*, ITC, ITU, UN Women, UNCTAD, UNDP, UNEP, UNESCO, UNFPA, UN-HABITAT, UNHCR, UNICEF, UNIDO, UNODC, UNOPS, UNRWA, UNU, UNWTO, UPU, WFP, WHO, WIPO, WMO, WTO, UNJSPF, OHCHR, WB. UNISSIG Observers: CERN, UNICC, PAHO, ADB, IADB, OPCW, OSCE, ICC, ESM, ICT-ILO, GF, CTBTO & ITC.

<sup>7</sup> Membership of the Working Group for Data and Cyber Risk WG includes: IOM\*, WIPO, ILO, UN Secretariat, UNV, UNICEF.

to be presented in the fall, aim to provide guidance on the procedural aspects on how to prepare and respond if needed to a ransomware incident.

#### Information Security at Meetings

Mr. Thomas Braun (UN Secretariat) presented on the risk of interception and surveillance of private conversations. Mr. Braun acknowledged the absence of a working group to report progress or updates on this matter, but emphasized the existence of prior incidents and the revelations brought forth by figures like Snowden, exposing widespread breaches and the unauthorized access to protected information. The presentation discussed the presence of individuals who engage in eavesdropping during meetings and stressed the need to address this issue. It emphasized the necessity of adjusting our behavior, particularly in our reliance on technology for communication. The availability of certain communication tools, such as Microsoft Teams with premium features, was mentioned as potentially being used by others for similar purposes. The presentation suggested measures for protection, including conducting regular bug sweeps, identifying any installed devices within office premises, and practicing digital hygiene to prevent the misuse of personal devices that could potentially collect information. Interestingly, the presentation noted the reluctance to consider the possibility of interception within home environments, despite a heightened level of awareness regarding surveillance.

#### Cybersecurity In Emergencies

During the UNISSIG last meeting in September 2022, the interest in establishing a special working group focused on cybersecurity in field and emergency situations was identified. In October 2022, the DTN agreed, leading to the establishment of an ad hoc working group chaired by UNHCR in December 2022, comprising nine agencies<sup>8</sup>.

The working group aims to develop a best practice guide for cybersecurity in emergencies based on an original submission from UNICEF. Additionally, they created a checklist or guide for a more trusted version of an internet café called the Secure Café Environment, building on the work of UNHCR and WHO.

Recommendations underlined that the preparations for emergencies and the Secure Cafe Approach be adopted in a broader UN context. The working group also proposed the establishment of a new working group to address cross-agency major security incidents. It emphasized that mutual trust should be explicitly recognized as a fundamental driver behind the UN wide cybersecurity baseline.

DTN took note of progress made by the working group on Cybersecurity in Field and Emergencies and approved the approach outlined within its paper; endorsed the specifications for pilot rollout in the UN in relevant locations and endorsed the creation of a new working group to address cross-agency coordination and alignment in multi-agency security incidents.

Updates on progress and planned deliverables for the UNISSIG working groups looking into guidance for Secure Messaging and Generic Human Resource Profiling for Cybersecurity positions were also provided by UNISSIG Co-Chairs.

---

<sup>8</sup> Membership of the UNISSIG WG on Cybersecurity in Emergencies included: UNHCR\*, UNICEF, CERN, EIB, IADB, IAEA, IFAD, UNESCO, UNOV, UNRWA, WFP, WHO & ICJ-CIJ.

## Cybersecurity Baseline

In December 2021, the cybersecurity baseline was introduced to fortify defenses against the mounting number of high-profile incidents, breaches, and cyber-attacks. A third iteration of this baseline was presented by Ng S. T. Chong (UNU), who led the working group<sup>9</sup> addressing its revision.

Version three of the baseline was introduced as entailing the following:

- Clarifying the baseline objectives and scope. This sets the context for interpreting and operationalizing the baseline.
- Establishing criteria to determine the inclusion of security practices or controls in the baseline. This addresses the question, How do we know if we are not raising the bar too high yet setting a bar high enough for a cybersecurity baseline?
- Reviewing and updating Version 2 in accordance with the defined objectives and inclusion criteria.
- Mapping the recommendations to recognized information security standards or best practices to facilitate evaluation and validation of the baseline.

On the strategic side, the cybersecurity program now incorporates secure SDLC considerations. Additionally, information security incident management has been expanded to encompass disaster recovery and management of audit logs. On the tactical side, the set of technical controls has been organized into four areas:

- Secure networks and systems
- Identity and privilege management
- Protecting data
- Security testing

The controls have been refined to align with the minimum baseline focus, balancing specificity and coverage. Furthermore, they now encompass network security, secure configuration, and mitigation measures addressing online security, data breaches, and supply-chain risks. This is a set of essential foundational security practices and controls that represent the minimum requirements for maintaining good cyber hygiene and constructing advanced defense that aligns with an individual organization's unique needs and risk profiles. The presentation covered key aspects of the cybersecurity baseline, including the addition of data protection and secure configuration in version 3. The discussion focused on the criteria for selecting security controls and practices, emphasizing their effectiveness, alignment with standards, and feasibility.

During the discussion, the topic of including Zero Trust in version 3 of the cybersecurity baseline was brought up. Concerns were raised regarding the associated costs and the need for careful consideration. The suggestion was made to use an online tool for self-assessment against the baseline and to explore automation and self-assistance to enhance it further. The consensus was to proceed with evaluating alignment with the baseline and measuring progress.

## Outcomes

- DTN approved the third iteration of the Cybersecurity Baseline (see Annex).
- DTN took note of the Risk Management Forum's subgroup White Paper on Ransomware.

---

<sup>9</sup> Membership of the UNISSIG Cybersecurity Baseline WG included: UNU\*, UNHCR, UNICC, IFAD, UNFPA, WMO, ICC-CPI.

- DTN requested UNISSIG to perform a survey amongst its members to measure adherence to the baseline and the cybersecurity maturity of organizations.
- Organizations were recommended to develop a phased introduction to Zero Trust security, starting with the discovery of identify high-value and high-risk assets.
- DTN endorsed the creation of a new UNISSIG working group to propose recommendations for physical and digital security controls to be implemented, to reduce the likelihood of sensitive information being compromised during and after sensitive meetings, including hybrid meetings.
- As an initial step towards increased security in cloud environments, organizations were recommended to segment (cloud-based) application environments.
- DTN noted the progress of the working group looking into Secure Messaging and will review UNISSIG WG deliverables during its autumn meeting.
- DTN noted the progress of the on Generic Human Resource Profiling for Cybersecurity positions and will be informed of WG deliverables during its autumn meeting
- DTN endorsed the creation of a new working group to address cross-agency coordination and alignment in multi-agency security incidents.

### Digital Advice to Member Countries

Herve Tourpe and Alok Kumar Verma discussed their work at IMF in providing advisory services in the field of technology and capacity development. They highlighted the creation of a unit within their organization to address the growing demand for technology-related assistance from member countries. They emphasized the collaboration between various departments, including the IT department, to deliver capacity development programs focused on digitalization and GovTech. They discussed specific initiatives such as hackathons and workshops organized in collaboration with the IT department to improve public financial management systems and promote data governance. They also mentioned successful partnerships with member countries in implementing digital solutions and highlighted the importance of unbiased guidance in navigating emerging technologies. The discussion showcased their effective collaboration, the impact of their work, and their commitment to providing quality services to member countries.

During the discussion, participants discussed topics related to partnerships, capacity building, cross-sectoral coordination, funding for IT initiatives, and innovation. They acknowledged the importance of collaboration and addressing the shortage of data scientists and cybersecurity experts. They also mentioned the need for capacity building in technical, policy, legislative, and citizenry spaces. The participants expressed interest in exploring collaboration opportunities and developing blueprints or journeys to guide their interventions. They discussed challenges in implementing digital solutions across sectors and the need for coordination between different organizations. Questions were raised about establishing innovation labs, funding mechanisms for IT initiatives, and resolving resource allocation issues. The participants shared their experiences and offered insights into their respective organizations' approaches.

### Global Digital Compact

Fayaz King (UN) provided insights on the work of the Envoy on Technology and referenced the Secretary General's previous session on leveraging digital technologies to accelerate progress on sustainable development goals. They emphasized that digital transformation is not just about technology but also about improving various aspects of life, such as food security, water, and sanitation. King then introduced the Global Digital Compact (GDC), which is an evolution of previous documents and statements on digital



cooperation. Mention was made of the upcoming policy brief, consultations, and the need for involvement from all actors, including states, non-state actors, the private sector, academia, civil society, and individuals. He highlighted the importance of respecting human rights, the rule of law, openness, inclusiveness, sustainability, security, and responsibility in the principles for GDC. He urged participants to engage in the remaining thematic sessions and make written submissions to ensure their voices are heard and reflected in the ministerial issues paper. The goal is to shape discussions, dialogue, and the eventual agreement on GDC by Member States.

## UN 2.0

Ayaka Suzuki (EOSG) and Kersten Jauer (EOSG) presented on the of UN 2.0, which is part of the Secretary General's Common Agenda. It aims to transform UN into a digitally oriented and globally relevant organization. The presentation emphasizes the need for cross-cutting capabilities in data, digital innovation, behavioral science, foresight, and futures thinking. The speaker discusses the gaps in knowledge and capacity within the organization and highlights the importance of the DTN in closing those gaps. They mention the progress made in areas like data, innovation, and digital transformation but acknowledge the varying capabilities across different organizations within UN. The presentation emphasizes the importance of practical use cases and concrete change to demonstrate progress and value to member states. The policy brief on UN 2.0 will be published in July, and the speaker invites feedback and collaboration from the DTN.

During the Q&A session, participants raised questions and comments regarding the measurement of success in UN 2.0, the challenges of funding and resource allocation, the incorporation of 2.0 in organizational strategies, and the need for talent and HR support. The speakers highlighted the importance of measuring impact and better delivering on the organization's mandate. They mentioned surveys and matrices as tools for measurement and emphasized the transformational nature of 2.0. Strategies were discussed to address funding challenges, including improving program offerings, advocating for more financing for data and digital projects, and exploring new financing instruments. The need for cross-cutting funding and resource mobilization within organizations was also mentioned. The speakers encouraged the inclusion of 2.0 in organizational strategies and highlighted the role of talent acquisition and training in driving change<sup>10</sup>. The importance of scalable and cost-effective training solutions was emphasized. Overall, the Q&A session focused on practical implementation, resource challenges, and the measurement of success in the context of UN 2.0.

## Balancing AI Risks and Opportunities

An engaging panel discussion took place on the risks and opportunities presented by AI. Moderated by Co-Chair Shirin Hamid, panelists included Anton Korinek (University of Virginia and Darden School of Business), Murielle Popa-Fabre (Council of Europe) and Michael Ibach (OICT).

Professor Anton Korinek addressed the great AI dilemma, discussing the potential winners and losers and the role of technology in maximizing benefits and minimizing risks. He mentioned the rapid growth of AI ChatGPT as the fastest growing app since its launch. He highlighted concerns about negative impacts such as job displacement and the use of AI for harmful purposes. He mentioned the call for a moratorium on the development of new AI systems and the need for risk-based regulation. The discussion also touched on the importance of governance, including topics like IP rights, transparency, and the need to address

---

<sup>10</sup> Results from a DTN Digital Transformation survey in October 2022, revealed that most (84.6%) respondents reference the United Nations Secretary-General's data strategy within their own ICT strategy.

misinformation. Mr. Korinek mentioned a survey revealing concerns about security and trust in AI. He then discussed the new paradigm of AI based on foundation models and the emergence of large language models. He highlighted the productivity effects of these models and the need to leverage them, particularly in developing countries. He predicted disruptions in labor markets and the need for governance to address the risks associated with AI. He also mentioned the potential for artificial general intelligence and the importance of being prepared.

Murielle Popa-Fabre discussed three key topics related to good governance and the workings of large language models like ChatGPT. The first topic explored the nature of words in the mind of ChatGPT and the importance of understanding its statistical language understanding. ChatGPT predicts the next word in a sentence based on probabilities calculated from organized words, rather than just grouping them as synonyms. The second topic focused on the attention mechanism, which plays a vital role in predicting sentences. Attention allows the model to emphasize certain words and determine their relevance in generating coherent sentences. Lastly, she delved into the concept of human intelligence and its connection to the brain area known as the hippocampus. Studies on taxi drivers highlight the importance of this region for spatial navigation and memory, demonstrating the need to maintain cognitive capital when implementing AI systems. Additionally, research shows that generative AI, like ChatGPT, can benefit less experienced or lower-skilled workers, leading to productivity gains. However, it's crucial to understand the shift in tasks and ensure that human competencies and capital are not lost.

During his presentation, Michael Ibach, who is the chief of policy and compliance in the OICT (UN Secretariat), provided an update on their work regarding the principles of ethical AI and its implementation. He mentioned that the media is increasingly focusing on the risks associated with AI, and he highlighted the recent departure of Geoffrey Hinton from Google, which has gained significant coverage. He emphasized the importance of governance in AI and mentioned a survey by Gartner that confirms the concerns about the governance of AI, especially generative AI. He discussed the need for regulatory measures and mentioned the EU AI act as a significant development. However, he also acknowledged the challenges of regulating generative AI effectively. He emphasized the need for self-regulation by organizations and providers of foundation models. He mentioned the principles of ethical use of AI established by the UN and UNESCO, and the adoption of these principles by the HLCF. He described their organization's approach to turning these principles into practical policies, including the development of a policy on responsible AI use and a playbook for responsible technology. He also mentioned the challenges of keeping up with the rapidly evolving AI space and the international regulatory landscape. Additionally, he discussed the development of toolkits and API services to enable and govern the adoption of advanced data analytics technologies. He highlighted the importance of building awareness and skills within the organization and mentioned a program called Unite Academy that aims to enhance data skills and create awareness around underlying technologies. Overall, he provided an overview of the initiatives and strategies employed by their organization to implement ethical AI principles and strengthen governance in AI usage.

The discussion revolved around various topics related to AI and its impact on society. One participant asked about the possibility of taxation on technological progress that benefits certain factors at the expense of labor, which could contribute to the development of universal basic income and create a future where everyone benefits. Another participant raised questions about evaluating the quality of AI systems, aligning AI with human values, and the role of data governance in AI development. The conversation also touched on controlling fake news and combating hate speech and misinformation using AI. The speakers

discussed the need for benchmarks and representative data, as well as the importance of global governance and alignment with human cognitive processes. The session concluded with further discussions on aligning AI with human values, implementing norms, and the potential for mixed systems that combine symbolic representation with statistical approaches.

#### Outcomes

The importance of a common approach and collaboration within the group was highlighted in discussions. Members agreed to address generative AI together to arrive at a common position and develop recommendations.

- A virtual meeting is to be scheduled in the short term to arrive at a common position and provide recommendations on the topic of Generative AI at the workplace. CEB Secretariat to draft and circulate a paper (based on member input) for review beforehand, to be further refined and finalized during the virtual meeting.

#### NASA's Digital Transformation Journey

Ms. Marlowe (Digital Transformation Officer, NASA) and Jeff Seaton (CIO, NASA) presented on NASA's digital transformation journey. The presentation opened by defining digital transformation as a radical change that makes processes, products, or capabilities unrecognizable from their previous form. They acknowledge the interdependence between digital transformation (DT) and information technology (IT) while clarifying their differences.

The motivation behind NASA's pursuit of digital transformation is attributed to the increasing complexity of missions, evolving partnership landscape, changing expectations, affordability concerns, transparency demands, and inclusivity expectations. To make the concept of digital transformation relatable, the presenters create personas representing individuals at NASA. These personas illustrate the potential impact of transforming the way they work. Examples include a scientist, an employee in a mission support function, and an operator in a laboratory. The personas depict the digital aspects of their future experiences. The presenters acknowledge the challenge of engaging employees focused on meeting milestones and deadlines, stressing the need to make digital transformation strategically important and appealing. The presenters discussed the listening tour conducted with senior leaders to identify areas for transformation. This led to the identification of four transformation targets: transforming engineering development, transforming discovery, transforming decision making, and transforming operations. They highlight the interconnectedness of these targets and the need for collaboration across NASA.

Five digital levers were introduced as essential focal points: interoperable architectures, process transformation, data foundation, tools rationalization, and strength in inclusive teaming. These levers provide a methodology for organizations to follow, ensuring effective utilization of digital advances in achieving transformation goals. The presenters emphasize considering people, geographic inclusivity, and organizational inclusivity throughout the transformation process. The focus then shifted to technology foundations that NASA considers ripe for adoption to address their business challenges. These foundations include intelligent automation, generative AI, extended reality, model-based engineering, zero trust, secure cloud, and high-performance computing. The presenters stress the interconnectivity of these technologies and the importance of understanding their impact on various functions. The desired outcomes of the digital transformation efforts are identified as seamless partnering, navigating complexity, agility in processes, tackling affordability and sustainability, ethical and transformative AI, innovation in future missions, and inspired and engaged citizens. These outcomes go beyond digital

adoption and serve as indicators of successful transformation. The presentation concluded by summarizing the strategy's key components, including the transformation targets, digital levers, technology foundations, and mission outcomes. The implementation strategy involves igniting a common transformation vision, defining roadmaps, identifying near-term priorities, and engaging individual organizations in determining their roles and contributions.

During the discussion, participants praised the presentation and raised questions about incentives for embracing digital transformation, setting priorities in complex organizations, measuring progress, and generating value from data in the public sector. NASA highlighted initiatives such as incorporating digital transformation into performance plans and gaining agency-level leadership engagement. They also discussed concepts like digital twinning and the importance of streamlining processes before automation. Strategies to accelerate digital transformation were explored, emphasizing senior-level support, aligning priorities, and engaging early adopters. The significance of data culture, common platforms, and tools for data analytics were underscored. The conversation reiterated the importance of business-led transformation, the challenges of integrating horizontal and vertical transformation currents, and the value of collaboration and partnerships. Governance structures, including centralization versus a federated approach, were discussed, with senior leadership support and a clear strategic vision highlighted as crucial. The role of the CIO as a strategic advisor and the need for cultural change, effective organizational structure, and managing expectations were also addressed. The example of creating a multi-mission, multi-cloud environment was cited as a means to foster collaboration and integration among engineering teams.

### Digital Transformation in the UK Government

Will Joss and Angus Montgomery, who hold positions at the Central Digital and Data office, discussed their experience of implementing a digital strategy at scale within their country. They emphasized the importance of effective digital transformation and the need for a stronger central agency to lead government-wide efforts. Their department's responsibilities include setting strategic directions, establishing standards, and building digital skills. They recognized the challenges faced in previous attempts and stressed the need to learn from past experiences. Their vision for a transformed digital government by 2025 includes missions such as improving public services, implementing a single login system, enhancing data utilization, ensuring secure technology, promoting digital skills, and supporting digital transformation. The strategy focuses on securing high-level support from government officials and incorporating measurable commitments with clear goals to achieve by 2025. Collaboration and coordination among government departments are highlighted as crucial for success.

The Q&A covered various topics, including the concept of "digital by default" and how it is tracked as a key performance indicator (KPI), the approach to adjusting pay scales to attract talent, the challenges of data quality and its impact on decision-making, the management of cultural change within the digital office, the volume and interfaces of services provided, and the future of the tech envoy's office and collaboration with the UN. The speakers addressed these questions, highlighting the importance of driving a culture of transformation and innovation, the need for a comprehensive digitalization process, the complexities of addressing pay disparities compared to the private sector, the challenges of scaling digital services and APIs, and the significance of training senior leadership in digital skills. They also discussed the strategies for retiring legacy systems, the use of data-driven insights, and the collaborative efforts to strengthen partnerships, funding, training, and skills development within the UN.

## The Role of Chief Digital Officer

While it is generally observed that the role of CDO focuses on digital strategy, transformation, data analytics, and emerging technologies and the purview of a CIO is commonly defined as internal IT operations and infrastructure, within the UN system the role of CIO is seen to combine both functions in most cases. Results of a pre-meeting survey undertaken within the DTN revealed that the position of CDO is the exception and not the rule.

The survey<sup>11</sup> revealed that 75% of organizations already have a digital transformation strategy in place, while 20% are still in the process of developing one. The survey also revealed that 65% of respondents have a digital transformation agenda that is oriented towards both internal activities and external beneficiaries, while 30% focus primarily on internal activities. The top three challenges identified by the respondents were funding and resources (80%), change management and culture (75%), and availability of knowledge and expertise (35%). As for the actions considered most beneficial for advancing the digital transformation agenda, 50% of respondents highlighted sharing best practices and innovations, followed by enhancing governance and strategy oversight (40%), and improving processes (35%). In terms of maturity, 80% of organizations reported that their digital transformation efforts were growing (45%), maturing (15%), or fully mature (20%). Funding mechanisms for digital transformation initiatives varied among the entities, with 20% relying on dedicated and regular program funding, another 20% utilizing a combination of dedicated extra-budgetary funding and existing resources, and an additional 20% employing a combination of all funding sources. 15% relied solely on existing resources, and another 15% relied exclusively on extra-budgetary funding.

In previous DTN meetings it has been noted that one challenge is that the CDO title is defined inconsistently across organizations (an observation shared by Gartner within industry at large), and that a coherent understanding of CDO responsibilities (as well as the future of the CDO role) would go far to support effective partnerships. In order to facilitate a common understanding, representatives from four DTN organizations where this role, or similar, is in place (as distinguished from the CIO role), were invited to share their views and experiences with the Network.

Robert Opp (UNDP) shared UNDP's experience with digital transformation. He explained that the organization recognized the need to embrace digital technology and developed a digital strategy in 2019. The strategy aimed to understand and leverage digital trends to support development efforts. The COVID-19 pandemic accelerated the demand for digital support from UNDP's country partners, leading to the revision of the digital strategy and its integration into the organization's strategic plan. The strategy is guided by principles such as human rights, inclusivity, and open digital frameworks. It focuses on three objectives: digitally enabled programming, supporting national digital transformation efforts, and developing internal digital capabilities. He briefly discussed each objective, emphasizing the importance of embedding digital solutions in thematic areas, assisting countries in inclusive digital transformation, and fostering a digitally native culture within the organization. His presentation highlighted the significance of digital ecosystems, strategic approaches, and a rights-based, inclusive approach to digital development.

Sally Radwan Golestan (UNEP) discussed the digital transformation and sustainability efforts of UNEP. Sally, the Chief Digital Officer, explained that UNEP aims to harness technology for sustainability while

---

<sup>11</sup> Undertaken by OICT in preparation for the meeting, the survey was completed by 20 DTN member organizations, representing the majority.

ensuring that technology itself is sustainable. She highlighted the environmental impacts of digital technology, such as energy consumption, water usage, and electronic waste generation. She also discussed the need to leverage digitalization for environmental monitoring, simulations, and behavior change towards sustainable practices. UNEP has adopted digital transformation as one of its main areas of work, focusing on data analytics and insights, convening partnerships, and capacity building. She plans to consolidate their digital solutions into a platform called the World Environment Situation Room. She emphasized the importance of user-driven approaches, digital governance, and product management. UNEP also collaborated with other initiatives and organizations to promote digital sustainability and influence policy agendas. They emphasized the need for sustainable digital transformation strategies that include environmental goals, data utilization, measurement of digital sector impact, and adherence to green standards.

Mike Walton (UNHCR) discussed the exponential growth in the number of forcibly displaced individuals and emphasizes the need to protect not only those displaced by war but also those affected by other factors like intimidation, violence, and sexuality. They mentioned the importance of digital inclusion and ensuring that communities have the skills and tools to engage in the digital world. They shared a story about the power of digital technology and its impact on changing lives. The presentation also touched on the organization's strategy, including refugee-facing objectives and internal objectives focused on improving efficiency and knowledge sharing. They highlighted the importance of co-designing solutions with the communities they serve and the significance of digital protection in addressing issues such as hate speech, misinformation, data protection, surveillance, and ethical use of technology. They discussed the need for effective digital communication and engagement with donors and partners, as well as the importance of digital advocacy and partnerships. The presentation also covered topics like capacity building, workforce planning, benchmarking, accessibility, and implementation at both regional and global levels.

The Network also heard from Friederike Schueuer (UNICEF), Global Chief of Data Policy, Analytics and Data Protection. Ms. Schueuer highlighted the need for integrating data and digital strategies, emphasizing that both are interconnected. She discussed the organization's role as a global custodian for SDG indicators and their focus on using data as a strategic asset. She mentioned the challenges of changing mindsets about data and the need to view it as enabling rather than something to be feared and explained the emergence of new types of data and the infrastructure and tools required to work with them, including data quality checks and automation. She also discussed the use of advanced technologies like machine learning and artificial intelligence, highlighting the need for increased computational power and new monitoring and versioning processes. The importance of partnerships and open-source alternatives in accessing data was emphasized and she acknowledged the risks associated with data misuse and the need for data protection and privacy policies that balance data use and protection. She also mentioned the challenges of working with different regulatory regimes and the politicization of data, promoting collaboration within the forum to address these issues and further the responsible use of data.

#### Common Denominators

Common themes and approaches emerged from all four speakers and included the need to embrace digital technology, adapt to the impact of COVID-19, set clear objectives, adhere to guiding principles, foster collaboration, promote digital inclusion, utilize and protect data strategically and ensuring an efficient implementation. All four speakers underscored the value of technology for development and sustainability and emphasized the need to adopt responsible data practices. The findings underscored the

significance of leveraging digital transformation to drive positive change and highlight the need for collective efforts in achieving sustainable and inclusive digital ecosystems.

## Breakout Sessions

Prior to the meeting's conclusion, breakout groups were created to consider the outcomes of this meeting and propose future courses of action. These groups were facilitated by Yoon Barker (UN), Barbara Nieuwenhuys (UN), Dino Cataldo Dell'Accio (UNJSPF) and Mike Walton (UNHCR). Under the direction of these facilitators, each group was invited to consider how best to effect digital transformation collaboration, strategies, challenges, measurement, and impact.

Discussions emphasized the importance of collaboration, transparency, and alignment towards common goals. It acknowledged the critical role of executive sponsorship and leadership in driving project success and the need for tangible deliverables to showcase the impact. Active participation, diverse perspectives, and finding common ground were valued, while gratitude was expressed to all participants. The discussion also highlighted the significance of showcasing tangible solutions to gain buy-in and stressed the importance of internal data literacy, capacity building, and staff training for successful transformation.

Consensus revolved around the themes of leadership driving change and enabling others to become change catalysts. The diversity of contexts, organization sizes, and teams was acknowledged, with the understanding that continuing the conversation would enhance confidence and knowledge sharing. Gratitude was expressed to the facilitators for their involvement. The need to wrap up the session and identify key takeaways, action items, and next steps for future meetings and organization-wide dissemination was discussed.

Breakout Group One discussed the successful collaboration and outcomes across chief digital data officers and CIOs. The conversation focused on envisioning the future and understanding the roles each individual brings to the table. The chief digital officer was seen as the driver of transformation, while the CIO focused on the digital dimension. The discussion emphasized the importance of partnership, with the CDO bridging the gap between programs and customer organizations, and the CIO integrating digital initiatives into IT roadmaps. The participants voted on the outcomes, highlighting the need for joint IT strategy, reference architectures, and a data lifecycle framework. The desired results included business transformation, actionable strategies, and forming teams to address high-impact challenges. The concept of shared vision and ownership in technology-driven transformation was emphasized, leading to improved insights and decision-making.

Breakout Group Two focused was on developing a cohesive and successful digital transformation strategy. The participants acknowledged the diverse models of collaboration between CDOs and CIOs and emphasized the importance of tailoring the approach to each organization's needs. They explored the temporary nature of the CDO role and the potential focus on change management rather than purely technology. Governance, organizational strategy, and digital strategy were identified as key factors in driving transformation. Incremental wins and a fit-for-purpose modernized digital organization were seen as positive outcomes. External themes like SDGs, climate change, and human rights were addressed, along with internal considerations such as the quintet of change and workforce digital literacy. The need for reducing duplication, promoting connected dialogue, and establishing a common funding strategy was highlighted. Data sharing, solutions catalog, and leadership's digital literacy were also mentioned as important aspects. The

group stressed the significance of clear roles, accountability, and a well-defined structure for enabling the strategy.

Breakout Group Three discussed the common challenges and opportunities in implementing digital strategies, including the need for change and embracing collaboration despite limited budgets. The importance of addressing leadership, resource capabilities, and structures as challenges was emphasized, while also identifying opportunities and quick wins. The discussion touched upon the need for organizations to stop certain practices, improve digital literacy, foster shared problem-solving, and explore private sector partnerships for pooled negotiations. Consensus decision-making and digitizing outdated processes were identified as areas that require improvement.

Breakout Group Four focused on measuring the impact and effectiveness of digital transformation initiatives. The consensus was on measuring the impact on beneficiaries, users, and member states, aligning with respective mandates and objectives. Productivity, efficiency, data quality, data-driven decision making, sustainability, new capabilities, member satisfaction (both internal and external), and interagency collaboration were identified as key areas to measure. The report suggested measuring process simplification, data quality indicators (accessibility, availability, timeliness, accuracy, relevancy, integrity, and security), output and outcome measurement, programmatic indicators for innovation, avoiding data duplication, staff satisfaction and retention, the ability to attract new staff, the impact on revenue generation, efficiency in delivering services, engagement and support from member organizations, collaboration maturity, unified engagement with external stakeholders, and measuring added value in services.

## Conclusions

The three-day meeting was considered intense but productive, with enriching presentations and discussions. The meeting concluded with expressions of gratitude and appreciation for the participants' contributions. The host organization, IMF, was praised for their exceptional hosting, and a team of colleagues behind the scenes was acknowledged for their support. The meeting was considered one of the best in the history of DTN, with a shift towards strategic discussions and member value. The Chairs were recognized for inspiring the agenda, and thanks were extended to the team who contributed to the success of the event.

### Communities of Practice

A Digital Transformation community of practice is to be established. This activity will be led by the existing DTN Digital Transformation WG. Attendees of the CDO workstream interested in leading or participating in this community are invited to contact CEB Secretariat. In addition, the following working groups are to be established:

- Digital Accessibility WG (Co-chaired by UN Secretariat & WHO)
- Open-Source Software WG (Co-chaired by UN Secretariat & UNFPA)
- Mutual Recognition WG (Chaired by UN Secretariat) - Members are invited to nominate themselves, or an organization representative, for the position of Co-chair.

In addition, OPCW was re-elected to lead the Collaboration Technologies WG for another two-year term.

A review of the naming convention applied to existing and new DTN working groups and special interest groups is to be undertaken and coordinated by CEB Secretariat.



### Future Meeting Format

During the meeting, there was a discussion about finding the best model for future meetings, possibly incorporating an online format. The focus was on allowing the agenda to drive the hybrid approach rather than just considering the number of days. While concluding, the Co-Chairs asked participants what topics should be included in future meetings. Members suggested focusing on breakout sessions, key performance indicators (KPIs), and network building. The participants agreed that maintaining a high level of content and incorporating both formal and informal networking opportunities was important.

Most participants (80%) expressed the preference for a DTN/CDO hybrid approach that combines separate and together sessions. The specific details of the hybrid format were discussed, including the possibility of having one day together and one day separate or organizing separate meetings for different roles within an organization. It was noted that the agendas of interest to CIOs and CDOs may vary. The need for an agenda-driven approach and maximizing value from the discussions was emphasized. Overall, there was a desire to create a meaningful and engaging agenda for the upcoming meetings.

It was concluded that annual DTN meetings will convene both (CIO & CDO) communities for partial session. Separate interim CDO sessions to be planned in parallel.

### Autumn Session Date and Venue

The next DTN session will be hosted in Nairobi by UNEP in the week of **27 Nov – 1 December 2023**. It will again be of duration three days (1 ½ days DTN, 1 ½ days for Digital Transformation CoP) and align with the UNICC MC. In addition, a field visit will be included.

### Autumn Session Agenda

Updates on the following topics are expected to be addressed by the agenda of the autumn session:

- Digital Transformation
- Generative AI
- Secure Messaging
- Ransomware
- Security at Sensitive Meetings
- Open-Source Software
- Digital Accessibility
- Mutual Recognition
- CRM/ERP

In addition, there was interest in maintaining a breakout segment, introducing key performance indicators (KPIs) for digital transformation and opportunities for network building, within and between both communities.

### Subsequent Sessions

The 2024 spring session will be hosted in Tokyo by UNU and be followed by a fall session, hosted by UNFCCC in Bonn.

### Virtual Session on AI

It was agreed to organize a virtual meeting on generative AI, as the topic was considered urgent. It was also recommended that the outcomes and recommendations emerging from the breakout sessions would be shared through the DTN report with HLCM and other bodies.

**A dedicated Teams session on AI is scheduled for July 6.**

While AI is a broader field encompassing various techniques for creating intelligent machines, generative AI, as a specific application of machine learning models to generate original content, will be the focus of this discussion.

The aim is to provide guidance that help organizations leverage benefits offered by AI, (including notably increased efficiency) while mitigating associated risks (including but not limited to adverse effects on data management, privacy and information security).

To facilitate the writing of a common position, members are encouraged to share related guidance and policies in advance (within the dedicated DTN meeting folder). An agenda and position paper will be circulated in advance of the meeting.

## Annex 1 – Agenda

**Digital & Technology Network (DTN) Spring Session (incl. CIO/CDO Session)****Agenda****IMF Headquarters, Washington D.C., 1-3 May 2023****Day 1 – Monday, 1 May (DTN Session)**

8h30		<b>Arrive at Security, Meet and Greet</b>
8h45	9h00	<b>Welcome</b> Deputy Managing Director, DMD Bo Li IMF Deputy Managing Director
9h00	9h10	<b>Opening of the Meeting &amp; Adoption of the Agenda</b> DTN Co-Chairs
9h10	10h15	<b>3 Strategic Technology Trends for CIOs to Watch</b> Marty Resnick, VP Analyst, Gartner <ul style="list-style-type: none"> <li>• Strategic technology trends have significant disruptive potential and set the stage for innovation over the next five years.</li> <li>• Enterprises must examine the business impact of these trends and adjust business operations appropriately or risk losing competitive advantage to those who do.</li> <li>• These are trends that IT cannot afford to ignore as they deal with the uncertainty driven by global change.</li> </ul>
	10h45	Coffee break
10h45	11h30	<b>CIO Priorities for 2023</b> Brian Jackson, Principal CIO Research Director, Info-Tech In this session, Info-Tech's Principal CIO Research Director, Bran Jackson will outline the five priorities that will help CIO's navigate the opportunities and risks of the year ahead. In examining the different capabilities that CIOs will require to succeed in the year ahead, it's apparent that a siloed view of IT isn't going to work. Just like a chess player in a competitive match would never limit themselves to only using their knights or their rooks, a CIO's responsibility is to deploy each of their pieces to win the day. While functional leaders may only see their next move, as head of the organization with a complete view of all the pieces, the CIO has full awareness of the board state. It's up to them to assess their gaps, consider the present scenario, and then make their next move.
11h30	12h00	<b>UN Maps</b> Kyoung-Soo Eom, OICT Diego Gonzalez Ferreiro, GSC Alexandre Caldas, UNEP, Chair of UN Geospatial Network  Outcome of the UN Maps Conference and a way forward to Deliver as One.

**Monday Afternoon (DTN Session)**

13h	13h45	<p><b>Intelligent Data Platform</b> Power BI / Synapse Customer Engagement Lead – PowerBI CAT Team – Microsoft Patrick LeBlanc – Principal Program Manager – Power BI CAT Team - Microsoft</p> <p>Microsoft's premier end-to-end data analytics platform, tailored to empower organizations with valuable insights and innovation. Our expert panel, featuring members from the Power BI and Synapse product groups, will engage in a comprehensive discussion on current and upcoming capabilities, including the evolution from predictive to prescriptive analytics. Additionally, Microsoft will unveil the latest product developments and cutting-edge industry news, ensuring relevance to organizational leadership seeking to stay ahead in the analytics landscape.</p> <ul style="list-style-type: none"> <li>20230420 DTN Survey - No-Code Platforms at Workplace.pdf</li> </ul>
13h45	14h30	<p><b>Microsoft 365 Copilot</b> Steve Gemmel – Technology Strategist – Tech for Social Impact Team - Microsoft</p> <p>A first look at how AI (Copilot) will be infused into Apps users use every day—Word, Excel, PowerPoint, Outlook, and Teams to unleash creativity, unlock productivity, and uplevel skills as you go through the day-to-day tasks. See how Business Chat will enable you to instruct these apps to create a first draft of an email or report, summarize a missed meetings or automate a process flow.</p> <ul style="list-style-type: none"> <li>20230420 DTN Survey - ChatGPT at Workplace.pdf</li> </ul>
14h30	15h15	<p><b>Digital Accessibility</b> High Level Review of ToR &amp; Deliverables Suzanne Shanahan, Chief Enterprise Application Center Americas, OICT</p> <p>Digital Accessibility Updates from ITU and WHO Edmund Tam, Head, Conference Technology Support Division, ITU (remote) Celine Hazbun, Head, Frontier Technologies and Data Information Management &amp; Technology, WHO (remote)</p> <p>Desirable outcomes:</p> <ul style="list-style-type: none"> <li>Approved ToR for Digital Accessibility working group.</li> <li>Agreement on approach proposed for establishing DA guidance and baseline.</li> <li>Initial membership.</li> </ul> <p>Documentation:</p> <ul style="list-style-type: none"> <li>20230424 DTN Sub-Group ToR Digital Accessibility.pdf</li> </ul>
15h15	15h45	<p><b>UN 2.0</b> Ayaka Suzuki &amp; Kersten Jauer (remote), EOSG UN 2.0 and next stages of digital transformation.</p>
15h45	16h00	Break
16h00	16h30	<p><b>Quantum</b> Sylvain St-Pierre, UNDP Desirable outcomes:</p>

		<ul style="list-style-type: none"> <li>Common understanding of the Quantum project, a multi-agency digital ERP services platform used by eight UN agencies.</li> <li>Awareness of new digital integration capabilities it provides and its potential role as an accelerator to digital transformation.</li> </ul> <p>Documentation: Quantum Computing.pdf</p>
16h30	17h30	<b>Plenary Discussion</b>
<b>Day 2 – Tuesday, 2 May (DTN Session)</b>		
9h	9h45	<p><b>Open Source and Developing Countries – Best Practices</b></p> <p>Panel Discussion, moderated by Herve Tourpe (IMF, Digital Advisory Unit Chief)</p> <ul style="list-style-type: none"> <li>Ben Cervený, Foundation for Public Code</li> <li>Lorena Cano, Inter-American Development Bank (IADB)</li> <li>Devesh Sharma, Gates Foundation</li> </ul> <p>Panel discussion on the adoption of open source and open access technologies in developing countries. Our expert panelists will examine the role of international organizations in promoting this transition and share their insights on the latest trends in government adoption of open source / access / data / knowledge. Using specific country examples, we'll explore the benefits and challenges of these technologies, and discuss best practices to help governments maximize their impact. This session will offer valuable insights into the future of open source and its potential to drive positive change around the world.</p> <p>Desirable outcome: Insights into the future of open source and its potential to drive positive change.</p>
9h45	10h30	<p><b>Zero Trust</b></p> <p>John Kindervag, Founder of Zero Trust</p> <p>Desirable outcome: consensus on major points, potentially including: Cybersecurity can be a major consideration when adopting cloud services. Cloud adoption can make it easier to implement zero trust security solutions.</p>
10h30	10h45	Coffee break
10h45	11h45	<p><b>DTN Working Groups - Status Updates</b></p> <ul style="list-style-type: none"> <li>ERPSIG - Massimiliano MERELLI (WFP), Marthinus Johannes Greyling (UNHCR)</li> <li>Cloud Working Group (FinOps) – Erzen Ilijazi (UN)</li> <li>Cloud Working Group (UN Private Cloud) - Francesca Duri (WIPO)</li> <li>CRM Working Group - Dino Cataldo Dell'Accio (UNJSPF)</li> <li>Open Source Software Working Group – Salem Avan (UN)</li> <li>Mutual Recognition Working Group - Tata Velayo (UN)</li> </ul> <p>Desirable outcomes:</p> <ul style="list-style-type: none"> <li>Approval of DTN working group proposed activities/deliverables.</li> <li>Approval of ToR for proposed new Working group (on OSS &amp; Mutual Recognition).</li> <li>New chairmanship for Communication Technologies WG.</li> <li>Review of DTN working group portfolio.</li> </ul> <p>Documentation:</p> <ul style="list-style-type: none"> <li>20230425 ERP Survey 2023 Summary.pptx</li> </ul>

		<ul style="list-style-type: none"> <li>• 20230426 DTN UN Private Cloud - Initial survey (for review only and not for submission).pdf</li> <li>• 20230224 DTN Sub Group Open Source Software (OSS) Group ToR.pdf</li> <li>• 20230329 Concept Note on Mutual Recognition in the Area of ICT - Draft v1.2.pdf</li> <li>• CEB.2023.HLCM.6.Rev.1 - Terms of Reference - HLCM Coordination Group on Mutual Recognition.pdf</li> </ul>
11h45	12h30	<p><b>UN Information Security Special Interest Group (UNISSIG) Updates</b> Sachiko Hasumi (IOM), Hans de Jong (IAEA)</p> <ul style="list-style-type: none"> <li>▪ Cybersecurity Baseline, Ng S. T. Chong (UNU)</li> <li>▪ Secure Messaging &amp; Ransomware, Sachiko Hasumi</li> <li>▪ Cybersecurity in Emergencies, Hans de Jong</li> <li>▪ Generic Human Resource Profiling for Cybersecurity positions, Hans de Jong</li> <li>▪ Cybersecurity protocols for sensitive UN meetings, Thomas Braun</li> <li>▪ Plenary discussion on UNISSIG recommendations, Sachiko Hasumi</li> </ul> <p>Desirable outcomes: In designing and implementing our digital strategies we should consider the security implications of using open source, zero trust, cloud adoption, and cybersecurity risks for ensuring that our digital and security strategies are aligned with each other. Other outcomes may include:</p> <ul style="list-style-type: none"> <li>▪ Common understanding on secure messaging.</li> <li>▪ Update on UNISSIG activities. Approval of WIP &amp; WG final outputs.</li> <li>▪ Approval of the cybersecurity minimum baseline revision.</li> <li>▪ Interest in joining WG on Cybersecurity protocols for sensitive UN meetings</li> </ul> <p>Documentation:</p> <ul style="list-style-type: none"> <li>• 20230420 DTN Minimum Baseline for Cybersecurity - V3 Final Draft.pdf</li> <li>• 20230301 UNISSIG Ransomware White Paper - Draft.pdf</li> <li>• 20230419 Cybersecurity in Field and Emergencies.pdf</li> <li>• 2023-5 UNISSIG Status Update for DTN.pptx</li> </ul>
12h30	13h	<p><b>Conclusions &amp; Wrap-Up</b> DTN Co-Chairs</p> <ul style="list-style-type: none"> <li>▪ Review of draft conclusions and recommendations</li> <li>▪ Date and venue of next session (Fall session in Nairobi proposed)</li> <li>▪ AOB</li> </ul> <p>Closure of DTN session (Part 1 of 2)</p>
	13h	Lunch
<b>Tuesday Afternoon (CIO/CDO Session)</b>		
14h	14h10	<p><b>Opening of the DTN CDO-CIO Session</b> DTN Co-Chairs</p>
14h10	14h45	<p><b>Digital Advice to Member Countries (Lessons Learned from the IMF)</b> Herve Tourpe (IMF) remote, Alok Kumar Verma (IMF)</p>

		Desirable outcomes: Capitalize on the IMF lessons learned on digital advice to member countries, with regard to: <ul style="list-style-type: none"> <li>▪ Responding to the growing need for guidance on digitalization in the Least Developed Countries.</li> <li>▪ Building capacity for the implementation of digital initiatives</li> <li>▪ Coordinating across international organizations</li> <li>▪ Role of IT Departments in supporting member countries</li> </ul>
14h45	15h	<b>Global Digital Compact (GDC)</b> Fayaz King, Office of the Secretary-General's Envoy on Technology (OSET) Desirable outcomes: Achieve a common understanding about the key principles of the Global Digital Compact, based on: Respect for human rights; Rule of law; Openness and inclusiveness; Sustainability; Security; Responsibility
15h	15h15	Coffee break & family photo
15h15	16h	<b>Digital Strategy Best Practices (UK Government)</b> Will Joss, Head of Strategy, Central Digital and Data Office, Cabinet Office (remote) Angus Montgomery, Head of Strategic Projects, Central Digital and Data Office, Cabinet Office (remote)  Learn from the experience of the UK's Central Digital and Data Office in designing and implementing the UK Government's Digital, Data and Technology strategy.
16h	16h45	<b>The Great AI Dilemma - Balancing AI Risks and Opportunities</b> Anton Korinek (in-person): Rubenstein Fellow, Brookings and Professor of Economics, University of Virginia and Darden School of Business Murielle Popa-Fabre (remote), Expert on Machine Learning and Natural Language Processing, Council of Europe Michael Ibach, Coverage of HLCP IAWG-AI Principles  <ul style="list-style-type: none"> <li>• 20230420 DTN Survey - ChatGPT at Workplace.pdf</li> </ul>
16h45	17h15	<b>Plenary Discussion</b> , moderated by Shirin Hamid, IMF CIO Desirable outcome: Recommendation for the CEB on AI.
17h15	17h45	<b>Plenary Discussion</b> , moderated by DTN Co-Chairs Desirable outcomes: Review of initial observations and recommendations
	17h45	<b>Closure</b>
	19h00	<b>Dinner</b> La Vie, 88 District Square SW, Washington, DC 20024. <u>Shuttle buses from HQ1 at 18h30</u> Return between 21h15 – 21h45  Thank you for confirming interest in attending dinner on Tuesday ASAP to: Lillian Chand LChand@imf.org

**Day 3 - Wednesday 3 May (CIO/CDO Session)**

9h	10h	<p><b>NASA's Digital Journey</b>  Ms. Marlowe, Digital Transformation Officer, NASA  NASA is not only seeing back to the origins of the universe with the Webb telescope, but also actively transforming itself to deliver even bolder missions in an ever more digitally-enabled, hyper-connected, fast-paced, and globally-competitive world. With their revised Digital Transformation (DT) Strategic Framework released in late 2022, NASA has charted a path to transform its work, workforce and workplace, to enable new approaches to engineering, scientific discovery, program/project management decision making, and business operations. The DT strategy is being brought to life by creating community-owned roadmaps that guide individual organizational investments and decisions within NASA's federated operating model.</p> <p>Desirable outcomes:  Learn from the experience of NASA's multi-year effort to transform the agency's operations and culture using digital technologies to:</p> <ul style="list-style-type: none"> <li>▪ Accelerate the pace of innovation</li> <li>▪ Empower the workforce</li> <li>▪ Engage the public</li> </ul>
10h	10h20	<p><b>UNDP:</b> UNDP's Digital Strategy and transformation - Robert Opp, Chief Digital Officer / Sylvain St-Pierre, CIO / Gayan Peiris, Senior Digital Leader  Desirable outcome: Learn from the experience of UNDP's digital transformation journey in:</p> <ul style="list-style-type: none"> <li>• Developing the overall vision and strategic objectives of the Digital Strategy 2022-2025 based on our experiences and observations</li> <li>• Supporting the development of inclusive and rights-based digital ecosystems</li> <li>• Embedding an agile and innovative culture, with a digitally-competent workforce</li> <li>• Developing fit-for-purpose digital infrastructure, systems and processes for the organisation</li> <li>• Leveraging data as strategic assets</li> </ul>
10h20	10h40	<p><b>UNICEF:</b> Friederike Schueuer, Global Chief of Data Policy, Analytics and Data Protection  Desirable outcomes: Learn from the experience of UNICEF in:</p> <ul style="list-style-type: none"> <li>▪ Developing and implementing a data policy aligned with UNICEF's values and principles.</li> <li>▪ Ensuring that UNICEF's data is collected, used, and shared in a responsible and ethical manner.</li> <li>▪ Protecting UNICEF's data from unauthorized access, use, or disclosure.</li> <li>▪ Promoting the use of data to improve UNICEF's programs and services.</li> <li>▪ Building capacity within UNICEF on data management and use.</li> </ul>
10h40	11h00	Coffee break
11h00	11h20	<p><b>UNEP:</b> Sally Radwan Golestan, Chief Digital Officer  Desirable outcomes: Learn from the experience of UNEP in:</p> <ul style="list-style-type: none"> <li>▪ Developing and implementing a digital strategy for UNEP aligned with the organization's strategic plan.</li> <li>▪ Ensuring that UNEP's digital capabilities are aligned with its needs and priorities.</li> <li>▪ Promoting the use of digital technologies to improve UNEP's work.</li> <li>▪ Building capacity within UNEP on digital technologies.</li> <li>▪ Collaborating with other UN agencies and partners on digital initiatives.</li> </ul>



11h20	11h40	<b>UNHCR:</b> Mike Walton, Head of Digital Services Learn from the experience of UNHCR in: <ul style="list-style-type: none"> <li>▪ Providing digital services that support the UNHCR's mission to protect and assist refugees.</li> <li>▪ Ensuring accessibility and user-friendliness.</li> <li>▪ Promoting the use of digital technologies to improve the lives of refugees.</li> <li>▪ Building capacity within the UNHCR on digital technologies.</li> <li>▪ Collaborating with other UN agencies and partners on digital initiatives.</li> </ul>
11h40	12h30	<b>Plenary Discussion</b> Desirable outcomes: <ul style="list-style-type: none"> <li>▪ Common understanding of the CDO function within operational and programmatic contexts.</li> <li>▪ Common denominators identified, on which to build a platform for future coordination between CDO &amp; CIO communities</li> </ul>

### Wednesday Afternoon (CIO/CDO Session)

13h30	14h00	<b>DTN Working Group on Digital Transformation</b> Dino Cataldo Dell'Accio (UNJSPF) Presentation of the work conducted by the working group: Desirable outcome: Approve the progress and suggestions of the DTN – Working Group on Digital Transformation on definitions, KPIs, risks, and best practices Co-Chair and establishment of CoP
14h00	16h45	<b>Break-out Sessions</b> Moderated by Yoon Barker (UN) & Barbara Nieuwenhuys (UN)  Some of the common challenges that prevent collaboration between CDOs and CIOs include having different priorities; backgrounds; cultures; and metrics. Working in groups, the following themes will be discussed: <ol style="list-style-type: none"> <li>1. High-level expectations of each other's roles and responsibilities (CDOs &amp; CIOs)</li> <li>2. Potential approaches to improve collaboration between CDOs &amp; CIOs</li> <li>3. Potential indicators of a "successful" collaboration between CDOs, CIOs, and Other Stakeholders (i.e., Representatives of Substantive Officers; Official Counterparts; etc.)</li> <li>4. Potential indicators of a "successful" implementation of Digital Strategies</li> </ol> <p>It is recognized that that no one-size-fits-all and the best digital strategy for an organization will depend on a variety of factors, including the organization's size, mandate, resources, and budget. The outcomes of this discussion may consider the need for organizations' digital strategies to:</p> <ul style="list-style-type: none"> <li>▪ Constantly evolve. The digital landscape is constantly changing, and organizations need to be able to adapt their strategies accordingly.</li> <li>▪ Focus on providing value to our "beneficiaries" (official counterparts; end-users; clients). We need to use digital technologies to create services that meet the needs of our clients.</li> <li>▪ Integrate with our overarching organization strategy. Digital technologies should be used to support our organization's overall mandates and goals.</li> </ul>

16h45

17h30

- Be rooted on data, analytics, and KPIs. We need to use data to track – and KPI to measure - the effectiveness of our digital strategies and make necessary adjustments.

Desirable outcomes:

- Practices to adopt or drop in Digital Transformation, cybersecurity & capacity.
- Recommendations for ongoing collaboration between CDOs and CIO communities

### **Conclusions and Closure**

DTN Co-Chairs

- Key findings, recommendations and priority actions
- Closure

## Annex 2 –Participants

The following list of participants excludes external presenters and provides a basis for the formation of a new community of practice on Digital Transformation.

Agency	Name	Position
<b>FAO</b>	Dejan Jakovljevic	CIO
<b>GCF</b>	Imai Jen-La Plante	Principal Data Scientist
<b>GSC</b>	Diego Gonzalez Ferreiro	Information Systems Officer
<b>IAEA</b>	Rola Khreis	Acting CIO
<b>IAEA</b>	Hans de Jong	CISO, Co-Chair UNISSIG
<b>ICAO</b>	Bertrand Frot	Chief Information Officer (CIO) and Deputy Director Information Management Services
<b>ICAO</b>	Sanya Dehinde	Chief, Information and Communication Technology Section
<b>ICJ</b>	Alvaro Flores Diaz	Head of ICT Division
<b>IFAD</b>	Thomas Bousios	Director, ICT Division
<b>IMF</b>	Bo Li	Deputy Managing Director
<b>IMF</b>	Shirin Hamid	CIO
<b>IMF</b>	Pierre Passin	Deputy Director and Chief Technology Officer. IT Department
<b>IMF</b>	Magi Clavé Badia	Deputy Director and Chief Digital Products. IT Department
<b>IMF</b>	Ahmed Ammar	ICT Division
<b>IMO</b>	Vincent Jjob	Special Adviser to Secretary-General on Digitalization
<b>IOM</b>	Marietta Muwanga-Ssevume	Chief Information Officer and Director of ICT
<b>IOM</b>	Sachiko Hasumi	CISO, Co-Chair UNISSIG
<b>ITC</b>	Ivan Sequeira	Chief, Information Technology & Systems
<b>ITC-ILO</b>	Gaël Lams	Chief Information Officer
<b>ITU</b>	Anders Norsker	Chief, Information Services Department
<b>OHCHR</b>	Najah Didi	Head Enterprise Systems Unit, Information Management & Technology Section
<b>OPCW</b>	Dennis Cleary	Head of Information Services
<b>CEB</b>	Richard Maciver	DTN Secretary
<b>UN DGACM</b>	Barbara Schelkle	Chief Business Analysis Section
<b>UN DMSPC</b>	Yoon Barker	Chief of Service, Transformation, Analytics & Innovation
<b>UN DPO</b>	Barbara Nieuwenhuys	Director Digital Transformation
<b>UN DPPA</b>	Martin Waehlich	Chief Innovation Unit
<b>UN DPPA-DPO</b>	Avishan Bodjnoud	Chief Information Management
<b>UN DSS</b>	Unaisi Lutu Vuniwaqa	ASG, UN Department of Safety and Security

<b>UN DSS</b>	Esther Kuisch Laroche	Director, Partnerships and Specialized Support
<b>UN EOSG</b>	Ayaka Suzuki	Director Strategic Planning & Monitoring Unit
<b>UN EOSG</b>	Kersten Jauer	Deputy Director Strategic Planning & Monitoring Unit
<b>UN OCHA</b>	Suzanne Connolly	Chief Information Systems Mgmt
<b>UN OICT</b>	Erzen Ilijazi	Chief Technology Operations
<b>UN OICT</b>	Christina Goodness	Special Assistant to the CITO, OICT
<b>UN OICT</b>	Bernardo Mariano, Jr.	CITO
<b>UN OICT</b>	Salem Avan	Director, Policy, Strategy & Governance Division
<b>UN OICT</b>	Tata Velayo	Chief of Service, Information Systems and Telecommunications
<b>UN OICT</b>	Thomas Braun	Chief, Cybersecurity Service
<b>UN OICT</b>	Suzanne Shanahan	Chief, Enterprise Application Centre – Americas
<b>UN OICT</b>	Omar Mohsine	Information Systems Officer
<b>UN OICT</b>	Kyoung-Soo Eom	Chief of Section, Information Systems
<b>UN OICT</b>	Michael Ibach	Chief of Policy and Compliance Service, OICT
<b>UN OSET</b>	Fayaz King	Office of the Secretary-General's Envoy on Technology
<b>UN WOMEN</b>	Ismail Sabir	Manager, Business Applications
<b>UNCTAD</b>	Elena Tomuta	IT Chief
<b>UNDP</b>	David Jordon	Enterprise Application Portfolio Advisor
<b>UNDP</b>	Robert Opp	Chief Digital Officer
<b>UNDP</b>	Gayan Peiris	Advisor, Data, Technology and Digital
<b>UNEP</b>	Saiful Ridwan	Senior ICT Advisor, ICT Unit
<b>UNEP</b>	Sally Radwan Golestan	CDO
<b>UNEP</b>	Alexandre Caldas	Chair of UN Geospatial Network
<b>UNESCO</b>	Omar Obaig	CIO
<b>UNFCCC</b>	Kate McBride	Director
<b>UNFPA</b>	Soren Thomassen	Director, Information Technology Solutions Office
<b>UNHCR</b>	Doug Greene	CIO and Director, Division of Information Systems and Telecommunications
<b>UNHCR</b>	Mike Walton	CDO
<b>UNHCR</b>	Marthinus Johannes Greyling	ERPSIG Co-Chair
<b>UNICC</b>	Sameer Chauhan	Director
<b>UNICC</b>	NIETO BARRANTES Prado	Chief Business Relationship Management
<b>UNICEF</b>	Friederike Schueuer	Global Chief of Data Policy, Analytics and Data Protection
<b>UNICEF</b>	Chris Larsson	CIO
<b>UNICEF</b>	Kathleen Grady	Secretary
<b>UNIDO</b>	Jason Slater	CIO

<b>UNJSPF</b>	Dino Cataldo Dell’Accio	CIO
<b>UNOPS</b>	Tushar Dighe	CIO
<b>UNOPS</b>	Charlotte Tarp Toelle	Head of IT PMO
<b>UNOPS</b>	Kristina Egund	Head of ICT Delivery
<b>UNOSET</b>	Moritz Fromageot	ASSOCIATE EXPERT (OSET)
<b>UNRWA</b>	Kaan Cetinturk	CIO and Director of Information Management and Technology
<b>UNU</b>	Ng S. T. Chong	Chief of ICT and Director of Campus Computing Centre
<b>UPU</b>	Paul Donohoe	Digital policies and Trade Coordinator
<b>WFP</b>	Jay Mahanand	Chief Information Officer
<b>WFP</b>	Massimiliano MERELLI	ERPSIG Co-Chair
<b>WHO</b>	Biswamber Gurubacharya	Acting Chief Information Officer
<b>WIPO</b>	Karl Kalejs	CIO
<b>WIPO</b>	Francesca Duri	Chief Technology Officer
<b>WMO</b>	Katarzyna Ostrowska	Business Innovation and Digital Transformation
<b>WMO</b>	Rania Abou Chakra	Chief IT Division

## Annex 3 – DTN Minimum Baseline for Cybersecurity

Version 3 - 2023

In today's digital landscape, a minimum cybersecurity baseline is not a luxury or a matter of opinion, but an absolute necessity for any organization that wants to protect its assets, reputation, and stakeholders. The constantly evolving threat landscape and the increasing sophistication of cyber-attacks make it imperative for organizations to adopt a proactive approach to cybersecurity, including implementing a minimum baseline of security measures to ensure a foundational level of protection. Failure to do so could have grave consequences, including reputational damage, economic loss, legal liabilities, and compromised sensitive data. Therefore, it is crucial that all organizations, including UN agencies, recognize the importance of a minimum cybersecurity baseline and take concrete steps to implement and maintain it.

This new version preserves the structure and principles of the previous version and provides boundaries to ensure future revisions remain a minimum indispensable baseline, are viable for most UN organizations, and are effective against the most common threats.

The contribution of the new version is threefold:

1. Clarify the baseline objectives and scope.
2. Develop a shared understanding of the criteria behind the baseline recommendations.
3. Review and revise the baseline in the context of the set objectives, scope, and criteria.

This document represents the outcome of the UNISSIG Working Group tasked by the DTN with this revision.

### *Baseline Objectives*

Organizations across the UN system are in different states of cybersecurity maturity. With increased cross-agency collaboration, a common approach to evaluate each agency and each other's adequacy of foundational cyber protection mechanisms is increasingly important. The updated baseline is **not a comprehensive control set** for information security – rather it aims to support three objectives:

1. Establish a common set of minimum indispensable security practices and standards to promote mutual trust and ensure a foundational basis for **secure information sharing and collaboration** when accessing each other's systems or transferring data between agencies. This will help to reduce the risk of security breaches and foster efficiencies in inter-agency collaboration.
2. Enhance the **UN's collective reputation** by implementing a minimum baseline that ensures the protection of sensitive information and minimizes security incidents which could affect the reputation of the entire organization. This will help to safeguard the UN's credibility and reputation in the eyes of stakeholders, partners, and the public.
3. Encourage, and provide support and guidance to **less mature UN agencies** in developing and implementing cybersecurity measures, to help them make a strong business case to their executive management.

### *Scope*

The recommendations apply to all managed digital assets (insourced, outsourced and Software as a Service (SaaS), including information, networks, systems, processes, and applications), with the understanding that organizations must still address unique risk scenarios with specific mitigations above the recommended baseline. **It is a minimum, not a target.**

### *Rationale for Recommendations*

The team used five main criteria for security practices or controls selection for inclusion in the baseline:

1. **Applicability:** The minimum-security measures and practices should be technology neutral, sector agnostic, and independent of the organization's risk profile. They ensure that even the least mature and resource-constrained organizations can achieve a basic level of cybersecurity.
2. **Standards-based or best practices driven:** Each recommendation must be equivalent to, related to, or derived from existing widely accepted best practices or recommendations in at least one world-class information security standard.
3. **Effectiveness:** The recommendations should be effective in protecting the system or data from the most common threats (e.g., ransomware attacks, supply chain attacks, social engineering attacks, insider threats), but may not be sufficient against more advanced or targeted attacks.
4. **Usability:** The minimum baseline measures and practices are grounded in a balance between security needs and productivity needs. While strong security measures help protect against cyber threats, they can also make it more difficult for users to access systems and data, reducing productivity and impacting user satisfaction.
5. **Feasibility:** The recommendations should be feasible to most UN organizations to implement, maintain, and operate within the organization's overall budget, resources, and technical capabilities.

The set of controls presented are a necessary foundation for building more advanced and tailored security programs that meet the specific needs and risk profiles of each organization.

### *Adapting to Evolving Risks, Threats, and Best Practices*

*UNSSIG reviews the baseline annually or as required to account for changes in risks, threats, technology, and best practices.*

The updated security baseline remains structured in three top-level sections as in the previous version: the cybersecurity program, technical best practices, and information security incident management.

## **1. Cybersecurity Program**

Organizations should have:

- a) Defined cybersecurity governance and reporting.
- b) Explicit cybersecurity policies in place.
- c) A cybersecurity function, with clearly defined roles and responsibilities, that fulfils the second line of defense function for information security (as per CEB/2014/HLCM/14/Rev.1).
- d) Regular audit and assessment of the cybersecurity program's effectiveness to identify areas for improvement and ensure it remains up to date with the latest threats and best practices.

Organizations should have a security awareness process where:

- e) Security awareness training is included in onboarding and refreshed regularly for all users.
- f) Simulated phishing exercises are executed regularly.

Organizations should ensure that their risk management methodology:

- g) Explicitly includes cyber risk management.
- h) Includes a consistent vendor risk management approach with Procurement, including information security requirements in both vendor selection and on-going reviews or performance monitoring of suppliers supporting critical services.

Organizations should have a standardized, secure software development lifecycle where there is a requirement to develop custom applications.

## **2. Cybersecurity (Technical) Best Practices**

Organizations should maintain an inventory of digital assets (and vendors) and implement the following technical controls:

### **Secure networks and systems**

- a) Ensure organization-managed devices, systems, and applications are supported by vendors and are regularly updated. Appropriate risk mitigation controls, such as application layer firewalls must be implemented where legacy unsupported systems cannot be decommissioned.
- b) Harden managed devices, systems, and applications in accordance with vendor guidelines and industry best practice.
- c) Deploy prevention measures across managed workstations, backend systems, mail and web gateways to guard against malware and malicious websites.
- d) Apply network segmentation and network controls to restrict access to systems based on the principles of least privilege and need-to-know.



- e) Implement email security controls to mitigate the threat of domain spoofing - SPF should be implemented as a priority with a view to enabling DKIM and DMARC in future.<sup>12</sup>

#### **Identity and privilege management**

- f) Centralize identity and access management for all organization managed devices, systems, and applications through a directory service (or Single Sign On [SSO]).
- g) Enforce MFA (Multi-Factor Authentication) for all privileged user accounts and access to publicly exposed systems; implement a risk-based approach to determine when MFA is required for non-privileged user accounts, such as when accessing sensitive data.
- h) Restrict use of privileged (administrators) accounts – users should be provisioned standard user accounts for all activities unrelated to the admin role.

#### **Protecting Data**

- i) Identify and protect critical data with a backup plan.
- j) Use industry-approved encryption methods to protect sensitive data at rest and in transit.
- k) Dispose of sensitive data securely after its necessary retention period.

#### **Security testing**

- l) Perform regular vulnerability assessments on systems supporting business critical services.
- m) Perform regular independent penetration testing and/or red team testing, no less than once annually, in accordance with the organization's threat model.

### **3. Monitoring, Detection, Response, and Recovery**

Organizations should:

- a) Implement security solutions that monitor logs, aid auditing, detect potential threats, and facilitate rapid response to security incidents on managed digital assets.
- b) Establish an effective incident response plan, which may involve setting up a Security Operations Center (SOC) with skilled professionals to promptly identify, contain and mitigate the impact of a cyber-attack, whether in-house or outsourced.
- c) Maintain disaster recovery plans for critical systems to facilitate recovery from an incident.

---

<sup>12</sup> SPF is a standard email authentication method, which helps protect domains against spoofing and helps prevent outgoing messages from being marked as spam by receiving servers. DKIM is a standard email authentication method that adds a digital signature to outgoing messages. DMARC, which stands for "Domain-based Message Authentication, Reporting & Conformance", is an email authentication, policy, and reporting protocol.

## Cybersecurity Baseline Appendix – Alignment with Industry Standards and Best Practices

## 1. Cybersecurity Program

Organizations should have:

DTN Baseline	Standards, Guidelines or Best Practices	Implementation Control
a Defined cybersecurity governance and reporting;  b Explicit cybersecurity policies in place.	NIST CSF	Governance ID.GV-1: Organizational cybersecurity policy is established and communicated
	ISO/IEC 27014:2020 Information security, cybersecurity and privacy protection — Governance of information security	
	CIS Control #14: Security Awareness and Skills	14.1 Establish and Maintain a Security Awareness Program
	ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements	ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls
	CISA Cyber Protection Goals (CPG)	CPG common baseline goals 1 – 9: Account Security / Device Security / Data Security Governance & Training / Vulnerability Management / Supply Chain (Third Party)/ Resilience / Network Segmentation / Physical Security
c A cybersecurity function, with clearly defined roles and responsibilities, that fulfils the second line of defense function (as per CEB/2014/HLCM/14/Rev.1).	NIST Cybersecurity Framework	Framework functions for Identify, Protect, Detect, Respond, Recover
	NIST CSF	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and
	ISO/IEC 27014:2020 Information security, cybersecurity and privacy protection — Governance of information security	
d Regular audit and assessment of the cybersecurity	ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements	A5.4 Management Responsibilities
	NIST CSF	Implementation Tier 4: Adaptive

program's effectiveness to identify areas for improvement and ensure it remains up to date with the latest threats and best practices.	ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements	A5.35 Independent review of information security
--	--	--

Organizations should have a security awareness process where:

	<b>Standards, Guidelines or Best Practices</b>	<b>Implementation Control</b>
Security awareness training is included in onboarding and refreshed regularly for all users.	CIS Control #14: Security Awareness and Skills Training	4.1 Establish and Maintain a Security Awareness Program
	ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements	A6.3 Information security awareness, education and training
	NIST 800-171 Rev 2	3.2.1 Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.
Simulated phishing exercises are executed regularly.	CIS Control #14: Security Awareness and Skills Training	14.2 Train Workforce Members to Recognize Social Engineering Attacks
	ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements	A8.7 Protection against malware

Organizations should ensure that their risk management methodology:

	<b>Standards, Guidelines or Best Practices</b>	<b>Implementation Control</b>
Explicitly includes cyber risk management.	ISO/IEC 27014:2020 Information security, cybersecurity and privacy protection — Governance of information security	
	ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements	
	NIST CSF	
Includes a consistent vendor	CIS Control #15: Service Provider Management	15.2 Establish and Maintain a Service Provider Management Policy

risk management approach with Procurement, including information security requirements in both vendor selection and on-going reviews.	ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements	A5.1 Policies for information security
---	---	--

Organizations should have a standardized, secure software development lifecycle where there is a requirement to develop custom applications.

	CIS Control #16: Application Software Security	16.1: Establish and Maintain a Secure Application Development Process. 16.10 Apply Secure Design Principles in Application Architectures
	ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements	A14.2.6 Secure development environment (complete development cycle) A5.8 Information security in project management A8.25 Secure development life cycle A8.28 Secure coding
	NIST 800-171 Rev 2	3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.

## 2. Cybersecurity (technical) best practices

Organizations should maintain an inventory of digital assets (and vendors) and implement the following technical controls:

### *Secure network and systems*

	Standards, Guidelines or Best Practices	Implementation Control
Ensure organization-managed devices, systems, and applications are supported by vendors and are regularly updated. Appropriate risk mitigation controls, such as application layer firewalls must	CIS Control #2: Inventory and Control of Software Assets CIS Control #4: Secure Configuration of Enterprise Assets and Software CIS Control #7: Continuous Vulnerability Management CIS Control #16: Application Software Security	2.2 Ensure Authorized Software is Currently Supported 4.4 Implement and Manage a Firewall on Servers 4.5 4.4 Implement and Manage a Firewall on End-User Devices 7.3: Perform Automated Operating System Patch Management. 7.4 Perform Automated Application Patch Management 16.4 Establish and Manage an Inventory of Third-Party Software Components

be implemented where legacy unsupported systems cannot be decommissioned	NIST 800-171 Rev 2	3.7.1 Perform maintenance on organizational systems. 3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.
	ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements	A7.13 Equipment maintenance A8.1 User endpoint devices
b Harden managed devices, systems, and applications in accordance with vendor guidelines and industry best practice.	CIS Control #4, #16	4.1, 4.2, 4.6, 4.7 Establish a secure configuration process 15.7 Use Standard Hardening Configuration Templates for Applications
	NIST 800-53	CM-2 (7) Baseline configuration
c Deploy prevention measures across managed workstations, backend systems, mail and web gateways to safeguard against malware and malicious websites	CIS Control #10: Malware Defenses	10.1 Deploy and Maintain Anti-Malware Software
	NIST 800-171 Rev 2	3.14.2 Provide protection from malicious code at designated locations within organizational systems.
d Apply network segmentation and network controls to restrict access to systems based on the principles of least privilege and need-to-know.	ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements	A8.7 Protection against malware
	CIS Control #12: Network Infrastructure Management	12.2 Establish and Maintain a Secure Network Architecture
	CIS Control #4: Secure Configuration of Enterprise Assets and Software	4.4 Implement and Manage a Firewall on Servers
	ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements	A8.22 Segregation of networks
	NIST 800-171 Rev 2	3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts.
	CISA Cybersecurity Performance Goals	8.1 Network Segmentation

<p>Implement email security controls to mitigate the threat of domain spoofing - SPF should be implemented as a priority with a view to enabling DKIM and DMARC in future.</p>	CIS Control #9: Email and Web Browser Protections	<p>9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions</p> <p>9.5 Implement DMARC</p> <p>9.6 Block Unnecessary File Types</p> <p>9.7 Deploy and Maintain Email Server Anti-Malware Protections</p>
	NIST SP 1800-6 Domain Name System-Based Electronic Mail Security (Guidelines)	
	ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements	A8.7 Protection against malware
	CISA Cybersecurity Performance Goals	8.3 E-mail security

### ***Identity and privilege management***

	<b>Standards, Guidelines or Best Practices</b>	<b>Implementation Control</b>
<p>Centralize identity and access management for all organization managed devices, systems, and applications through a directory service (or Single Sign On [SSO]).</p>	CIS Control #5: Account Management	5.6: Centralize Account Management
	CIS Control #6: Access Control Management	6.7: Centralize Access Control
	ISO/IEC 27001	<p>A5.15: Access Control</p> <p>A5.16: Identity Management</p> <p>A5.18: Access Rights</p>
	NIST SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing	Section: 4.5 Identity and Access Management

<p>Enforce MFA (Multi-Factor Authentication) for all privileged user accounts and access to publicly exposed systems; implement a risk-based approach to determine when MFA is required for non-privileged user accounts, such as</p>	CIS Control #6: Access Control Management	<p>6.3: Require MFA for Externally Exposed Applications</p> <p>6.5: Require MFA for Administrative Access</p>
	NIST 800-171	<p>3.5.3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.</p> <p>3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.</p>
	ISO/IEC 27001	<p>A5.15: Access Control</p> <p>A5.18: Access Rights</p>
	CISA Cybersecurity Performance Goals	1.3 Multi-Factor Authentication

when accessing sensitive data.	NIST SP 800-207 Zero Trust Architecture	Section 4.5 Enterprise with Public- or Customer-Facing Services
		Section 5.3 Stolen Credentials/Insider Threat

Restrict use of privileged (administrators) accounts – users should be provisioned standard user accounts for all activities unrelated to the admin role.	CIS Control #5: Account Management	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts
	NIST 800-171	3.1.4 Separate the duties of individuals to reduce the risk of malevolent activity without collusion. 3.1.6 Use non-privileged accounts or roles when accessing non-security functions. 3.1.7 Prevent non-privileged users from executing privileged functions and audit the execution of such functions.
	ISO/IEC 27001	A5.3 Segregation of duties. A8.2 Privileged access rights. A8.3 Information access restriction.

**Protecting data**

	Standards, Guidelines or Best Practices	Implementation Control
Identify and protect critical data with a backup plan.	CIS Control #11: Data Recovery	11.1 Establish and Maintain a Data Recovery Process 11.2 Perform Automated Backups 11.3 Protect Recovery Data
	ISO/IEC 27001	A8.13: Information Backup
	CISA Cybersecurity Performance Goals	7.3: System Back Ups

Use industry-approved encryption methods to protect sensitive data at rest and in transit.	CIS Control #3: Data Protection	3.10 Encrypt Sensitive Data in Transit 3.11 Encrypt Sensitive Data at Rest
	NIST 800-171	3.5.10 Store and transmit only cryptographically protected passwords. 3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.
	ISO/IEC 27001	A5.10 Acceptable use of information and other associated assets A5.14 Information transfer A5.33 Protection of records
	CISA Cybersecurity Performance Goals	3.3 Strong and agile encryption
Dispose of sensitive data securely after its necessary retention period.	CIS Control #3: Data Protection	3.5 Securely Dispose of Data
	NIST 800-171	3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse.

	ISO/IEC 27001	A5.10 Acceptable use of information and other associated assets A5.33 Protection of records
--	---------------	--

**Security testing**

	Standard/Security Control/Guidelines/Best Practice	Implementation Control
Perform regular vulnerability assessments on systems supporting business critical services.	CIS Control #7: Continuous Vulnerability Management CIS Control #16: Application Software Security	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets 7.6: Perform Automated Vulnerability Scans of Externally Exposed Enterprise Assets 16.2 Establish and Maintain a Process to Accept and Address Software Vulnerabilities
	NIST 800-171	3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. 3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.
	ISO/IEC 27001	A8.8 Management of technical vulnerabilities
	CISA Cybersecurity Protection Goals	5.1 Mitigating Known Vulnerabilities
Perform regular independent penetration testing and/or red team testing, no less than once annually, in accordance with the organization's threat model.	CIS Control #16: Application Software Security CIS Control #18: Penetration Testing	18.1 Establish and Maintain a Penetration Testing Program 18.2 Perform Periodic External Penetration Tests 18.5 Perform Periodic Internal Penetration Tests 16.13 Conduct Application Penetration Testing
	ISO/IEC 27001	A8.8 Management of Technical vulnerabilities
	NIST 800-171	3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

**3. Monitoring, Detection, Response, and Recovery**

Organizations should:

	Standards, Guidelines or Best Practices	Implementation Control
--	---	------------------------



a Implement security solutions that monitor logs, aid auditing, detect potential threats, and facilitate rapid response to security incidents on managed digital assets.	CIS Control #8: Audit Log Management	8.1 Establish and Maintain an Audit Log Management Process 8.2 Collect Audit Logs 8.11 Conduct Audit Log Reviews
	NIST 800-171	3.3.1 Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.
	ISO/IEC 27001	A8.15 Logging
b Establish an effective incident response plan, which may involve setting up a Security Operations Center (SOC) with skilled professionals to promptly identify, contain and mitigate the impact of a cyber-attack, whether in-house or outsourced.	CIS Control #17: Incident Response	17.4 Establish and Maintain an Incident Response Process 17.5 Assign Key Roles and Responsibilities
	ISO/IEC 27001	A5.24 Information security incident management planning and preparation A5.26 Response to information security incidents A5.2 Information security roles and responsibilities
	NIST 800-171	3.6.1 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.
c Maintain disaster recovery plans for critical systems to facilitate recovery from an incident.	NIST CSF	PR. IP-9 Response plans