Task Team- evolution of WMO Information Systems (TT-eWIS)

Future Technology Workshop

Geneva 19-20th March 2019



## DISCLAIMER

**Regulation 43**

Recommendations of working groups shall have no status within the Organization until they have been approved by the responsible constituent body. In the case of joint working groups the recommendations must be concurred with by the presidents of the constituent bodies concerned before being submitted to the designated constituent body.

**Regulation 44**

In the case of a recommendation made by a working group between sessions of the responsible constituent body, either in a session of a working group or by correspondence, the president of the body may, as an exceptional measure, approve the recommendation on behalf of the constituent body when the matter is, in his opinion, urgent, and does not appear to imply new obligations for Members. He may then submit this recommendation for adoption by the Executive Council or to the President of the Organization for action in accordance with Regulation 9(5).

© World Meteorological Organization, 8 April 2019

The right of publication in print, electronic and any other form and in any language is reserved by WMO. Short extracts from WMO publications may be reproduced without authorization provided that the complete source is clearly indicated. Editorial correspondence and requests to publish, reproduce or translate this publication (articles) in part or in whole should be addressed to:

Chairperson, Publications Board

World Meteorological Organization (WMO)

7 bis, avenue de la Paix Tel.: +41 (0)22 730 84 03

P.O. Box No. 2300 Fax: +41 (0)22 730 80 40

CH-1211 Geneva 2, Switzerland E-mail: Publications@wmo.int

NOTE:

The designations employed in WMO publications and the presentation of material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of WMO concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

Opinions expressed in WMO publications are those of the authors and do not necessarily reflect those of WMO. The mention of specific companies or products does not imply that they are endorsed or recommended by WMO in preference to others of a similar nature which are not mentioned or advertised.

This or report is not an official publication of WMO and has not been subjected to its standard editorial procedures. The views expressed herein do not necessarily have the endorsement of the Organization.

# WIS 2.0 Future Technology Workshop Chair Report

WMO convened the "Future Technology Workshop" (19-21 March 2019, Geneva) . Participants included experts from WMO, industry (Amazon Web Services, EUROCONTROL, Google, Inmarsat, Microsoft, Motorola, Thuraya, and Wisekey), and standards organizations (International Telecommunications Union, Open Geospatial Consortium, and World Wide Web Consortium). The attendee list can be found on the workshop meeting page[[1]](#footnote-2). Representatives from private sector weather service providers were invited but unable to attend.

The aim of the workshop was to understand industry directions, determine alignment with the WIS 2.0 strategy and implementation approach[[2]](#footnote-3), and to prepare a summary statement for Cg-18 containing the conclusions of the WMO experts. The 2-day work plan can be found [online](https://wiswiki.wmo.int/tiki-index.php?page=eWIS-FutureTechhttp://wiswiki.wmo.int/tiki-download_file.php?fileId=5413)[[3]](#footnote-4). The following report provides a summary of key trends observed relevant to data sharing platforms, and identifies some of the risks and issues that may be encountered when operating in the cloud. This report is a supporting document for the concluding workshop statement to be submitted to Cg-18 for endorsement. The text of the statement is included in [Annex A](#_WIS_2.0_Future).

The workshop participants concluded that:

* The strategy for the evolution of the WIS and its implementation plan are fully in line with the technology industry trends for data-sharing.
* WIS 2.0 must be implemented as an agile system that is able to respond to technology industry changes.
* WIS 2.0 WIS 2.0 must prioritize an ongoing commitment to training and capacity building in all Regions to enable Members to effectively leverage industry supplied products and services; both free to use and paid for.

# Technology macro-trends relevant to data sharing platforms.

## Rapid advances in provision and uptake of cloud computing services.

'Big data' is simply described as "bigger than you have the capacity or capability to work with". Data volumes and the compute required for processing are rapidly outstripping the abilities of even the most advanced NMHS. Big data creates a paradigm shift in how we think about data sharing: as data becomes too big to move because of network capacity constraints, downloading data to one’s local compute environment for processing becomes untenable. Instead, we need to bring users’ processing ‘to the data’, enabling that processing to execute on the cloud-hosted compute environment in close proximity with the data.

Cloud computing provides an alternative option to continual investment in one's own infrastructure. It can be defined as on-demand availability of computer system resources (e.g. compute and storage). In the case of public cloud, access to these resources is delivered via the Internet with pay-as-you-go pricing.

Public cloud vendors are responding to the needs of the market - providing cloud platforms that enable their customers to build applications that scale to cope with 'big data' without them having to build, own or operate the underpinning infrastructure.

Illustrating the success of public cloud, Amazon Web Services (AWS) has grown from its inception in 2006 to a company with revenue of US$25B in 2018, while the Google Cloud Platform hosts 8 of the 10 'billion plus' user applications.

Public cloud vendors also provide free to use services, e.g. for sharing open data, where the vendor covers some, or all, of the infrastructure costs. Examples include AWS Public Dataset Program and Microsoft AI for Earth. The vendor's aim is to help customers to leverage the cloud to increase the value of their data through broader adoption and usage, and in doing so bring more users to their cloud platform. However, the lack of long-term commitment to vendors’ provision of free to use services may introduce risk to operations. Refer to section [2.3 Reliance on third-party service provision](#_Reliance_on_third-party) for further discussion.

Already there is widespread adoption of public cloud within meteorological domain. Examples include provision of access to real-time data (satellite imagery, radar etc.) where "the vast majority of activity on those datasets happens within the first second" following receipt of messages notifying subscribers that new data is available. Elsewhere, "Smallsat[[4]](#footnote-5)" operators are driving down operating costs by terminating their data directly into cloud-platforms where end-users can directly access those data, alleviating the need for expensive data-delivery gateways.

The Open Geospatial Consortium (OGC), an international non-profit standards development organization, recognizes that cloud is fundamental to how its 520 members and the global geospatial community want to share data. The OGC is working to evolve its open standards to make it easy to work with and share geospatial data in cloud environments.

The following trends are evident among public cloud offerings:

* Commoditisation of basic infrastructure services among public cloud vendors (e.g. elastic compute, object storage, notification etc.).
* Use of 'containers' (managed software environments similar to virtual machines) enables workloads (i.e. data processing, computation etc.) to be migrated between cloud platforms or even between cloud platforms and traditional 'on premise' infrastructure.
* Public cloud vendors will increase the number and geographic spread of 'regions' (i.e. resilient clusters of data-centres in a given geographic location) on their cloud platforms.
* Public cloud vendors use private backbone networks to provide reliable, high-speed transmission of data between their cloud platform regions.
* Public cloud vendors provide optimised hardware to support particular types of workload; e.g. HPC for numerical weather modelling, GPU for machine learning.
* Public cloud vendors will continue to invest heavily in data processing toolsets within their cloud platforms that aim to transform the way that customers work with big data, driving cost efficiencies and/or new business opportunities; e.g. artificial intelligence (AI) / machine learning, data cleansing / data integration, efficient query on petabyte-scale datasets etc.
* Market competition will continue to drive down the unit cost of offerings from public cloud vendors as they benefit from increasing economies of scale. For example, AWS have proactively reduced their prices over 70-times.
* Public cloud vendors will continue charge to move data off-cloud, between cloud-platforms, and even between cloud platform regions (i.e. 'egress costs') - these costs need to be factored into application operating costs.
* Public cloud vendors neither own data stored on their platforms nor take responsibility for performance of customer's applications deployed on their platform - although vendors will make a service commitment for provision of reliable infrastructure and help customers design 'fault-tolerant' applications.

It is important to note that WIS 2.0 does not require use of cloud platforms - public or otherwise. Members operating WIS Centres will need to decide whether deploying to a cloud platform is appropriate for their needs.

Cloud is a good fit for problems with certain characteristics, such as:

* Where applications need to flexibly scale, application operators only pay for capacity is used without up-front investment in massive infrastructure.
* Where organizations, particularly in developing countries, have neither access to sufficient IT infrastructure nor the workforce to maintain and operate that infrastructure.
* Where datasets are too big to move because of limited network capacity, users can work with data on the cloud platform (i.e. there is no need to download the data for local processing).
* Where cloud platforms provide data-processing/data-management toolsets that complement or enhance the capabilities of deployed applications.

However, operating in the cloud does not come without risk. Three topics for consideration of would-be cloud users are identified in section 2 [Cloud-based operations: risks and issues](#_Cloud-based_operations:_risks).

1. Lack of predictable operating costs.
2. Vendor-lock.
3. Reliance on third-party service provision.

Finally, readers should note that many of the participating experts referred to the concept of 'edge computing': where computational processing is embedded in sensor platforms and other connected devices (i.e. at the 'edge' of the network). Edge computing should be seen as a complement to cloud computing. It is commonly used in bandwidth-constrained environments to either reduce the volume of data that needs to be transmitted or where decisions or actions need to be made very quickly. For example, edge computing may be used to identify relevant artefacts from within high-volume data streams (i.e. image recognition processing within video); only notifications about those artefacts need be published, rather than the entire video stream. Computationally expensive data processing tasks, especially those that need to correlate data from multiple sources, remain good candidates for cloud-hosted workloads.

## Massive increases in Internet bandwidth, connectivity, reliability and security.

The Internet of Things (IoT) revolution is driving a massive increase in the numbers of connected devices and, in turn, the demand for increased network capacity. Industry is responding by providing massive increases in available bandwidth coupled with proportional reduction in like-for-like cost over the coming years. Network capacity constraints will become outdated within a few years - even for the most remote locations.

Network technologies are converging to provide ubiquitous connectivity - from close proximity (Near-Field Communication "NFC") to short-range (Bluetooth) to local-area networks (Wi-Fi) to wide-area networks (LTE, 5G, LoRa) to satcom for the remotest locations. Vendors are increasingly providing hybrid-network solutions complementing high-speed, low-cost connectivity where available with global coverage via satcom, e.g. LTE ground network combined with S-band satellite for the European aviation sector.

Widespread 5G rollout is anticipated by 2022, delivering enhanced mobile broadband with gigabit per second (Gbps), ultra-reliable, low-latency communications. Looking further out to 2030, the International Telecommunications Union (ITU) predict terabit per second (Tbps; 1Tbps = 1000Gbps), ultra-low-latency connectivity supporting near instantaneous availability of information across the world. The ITU note that new routing protocols may be needed to achieve these goals.

Innovation is also affecting satellite terminals and end-user devices. For example:

* Converged IP terminals with satellite and LTE functionality are now available for less than US$1000;
* Satcom chipsets have reduced in cost from US$100s to US$10s and are predicted to become low enough for inclusion in disposable devices; and
* Multi-megabit Ka-band satcom terminals have reduced in size from large diameter, fixed dishes to suitcase-size antenna that can be easily deployed in remote areas or emergency situations - or taken down in the event of severe weather.

In response to increasing threat, vendors are embedding increasingly sophisticated cybersecurity measures into the communications networks to protect data and remote assets. The ITU want industry to overcome reliability limitations of today's Internet - which will require a new approach to network design. They predict that the Internet of the future will be built on 'trustable network infrastructure'. Built-in security measures and will provide guaranteed delivery of information.

Service offerings from network providers are becoming increasingly flexible in response to changing market demands. For example, flexible weekly or monthly contracts are offered to the disaster response community.

Network providers are providing value-added services alongside network capacity to differentiate in an increasingly crowded market. For example, providing bespoke managed solutions for monitoring remote infrastructure, and pooling capacity from multiple network providers through a single marketplace to deliver the most cost-effective solutions to customers.

However, experts anticipate data volumes growing in parallel with network capacity. Big data will become even bigger and will remain difficult to quickly move between locations. Improvements in network capacity, reliability and connectivity will enable users to more effectively work and interact with big data at remote locations.

##  Use Web services to expose data and functions in distributed systems.

The Web is the World’s most successful vendor neutral distributed information system[[5]](#footnote-6). Since its inception, the World Wide Web Consortium (W3C) mission has been to "keep the Web open for everybody". Now 25-years old, with 460 members across US, Europe and Asia, the W3C continues to convene industry, government and research stakeholders to develop open standards for the Web, and ensure ongoing backward compatibility with today's Web.

Public cloud vendors, among others, recognise that the Web provides a stable platform upon which they can build their cloud offerings and deliver to customers.

Supporting interoperability in distributed systems, industry advocate exposing data and functions to users through APIs[[6]](#footnote-7) to abstract away from underlying implementation details.

EUROCONTROL also recognise this challenge. The core principles they define for the SWIM platform include use of a "service-oriented" approach - a technical way of saying that functions, including data access, are packaged into 'services' with clearly defined APIs.

With broad adoption of this API-centric approach, industry provide complementary off-the-shelf solutions that enable efficient and effective use of APIs to share data and functionality. These 'API Management' solutions provide the generic capabilities required for effective use of APIs such as user management, authentication and access control, gathering usage metrics and generation of statistics, controlled replacement of APIs with new versions, and even monetisation of API use through services marketplaces. API management solutions typically include a service catalogue describing all the APIs and services that are exposed and may provide a useful contribution to the WIS catalogue itself.

EUROCONTROL also include use of open standards as a core principle. The SWIM "Technical Infrastructure Profile", which defines the technical standards that will ensure interoperability within the SWIM platform; specifying standards to be used for both Web services and messaging protocols. This profile is broadly consistent with WIS 2.0 - albeit that the SWIM profile is more prescriptive about which open standards shall be used.

The mainstay of OGC activity is development of open standard Web service specifications and APIs for sharing geospatial data. With more than 10-years of cooperation between OGC and WMO, and the participation of NMHS in the standards development process, these OGC Web service and API standards are directly applicable in the meteorological and hydrological domains. Although the WIS 2.0 implementation approach does not define specific standards to use, OGC Web services and APIs are a good fit. These OGC APIs should enable meteorological and hydrological data to be readily shared with other domains and industry sectors.

# Cloud-based operations: risks and issues.

There are several risks and issues associated with cloud-based operations - particularly use of public cloud.

## Lack of predictable operating costs.

When operating in the cloud, one only pays for the infrastructure capacity that is actually used. This 'pay-as-you-go' business model will often deliver cost efficiencies when compared to operating one's own infrastructure. However, moving from an ownership model with well-known costs to rental model where both volume and unit prices are subject to change means that it is difficult predict operating costs.

Cloud vendors provide controls that can be used to cap or limit the amount of infrastructure capacity actually used, thereby protecting against unexpected peaks in costs. Cloud vendors also offer mechanisms to smooth out costs through peaks of troughs in demand. However, the costs will always be subject to a degree of variability. To mitigate this, customers will need to proactively review their infrastructure usage, optimising application deployments to minimise costs.

More challenging is that customers are subject to their vendor's pricing decisions. That said, it is unlikely that in a highly competitive market that vendors will increase their prices. As cloud vendors benefit from economies of scale, they will likely pass cost savings to customers. For example, AWS have proactively reduced their prices over 70-times.

However, the only sure way to mitigate against unaffordable price rises is being prepared to migrate to an alternative solution provider. See 'vendor-lock' below.

## Vendor-lock.

Vendor-lock (i.e. inability to change vendor) was identified as a key risk when deploying applications or storing significant volumes of data in the cloud. Several mitigation strategies that can be applied here.

When building applications for deployment in cloud platforms:

* Avoid exposing the platform's native services to end-users - use APIs, preferably open standard APIs, to expose application functionality. In this way, applications can be migrated to alternative cloud platforms without affecting end-users.
* Design your software around common (commoditised) capabilities of the cloud platforms where possible and modularise your software. In this way, it will be easier to swap out native services from one cloud platform for those of another.
* Deploy your application in a container (a virtualised software environment). Containers can be deployed on most cloud platforms as well as on your own infrastructure. In this way, your application(s) can be moved around as needed. Some public cloud vendors (e.g. Google) provide management tools to help manage container deployment in multi-cloud environments.

All public cloud vendors charge to move data off-cloud: exporting petabyte-scale archives from a public cloud platform will be costly. The best solution is to have another copy of the data - perhaps in an on premise tape archive, or even hosted within another cloud platform. Although there is a cost to maintaining a copy, these are low (e.g., Microsoft Azure provides 'deep-cold storage' at US$0.02 per TB per month). Alternatively, make sure that you have contractual arrangements that enable physical means to export data from the vendor's facilities. Most cloud vendors provide “physical data transport appliances" to move data to/from cloud-vendor's data centres - from suitcase-sized storage devices upwards (e.g. AWS Import/Export Snowball[[7]](#footnote-8) with a capacity of 50TB).

## Reliance on third-party service provision.

Cloud-based applications are entirely dependent on the infrastructure services provided by the cloud platform. Effectively, one becomes reliant on third-party infrastructure. Public cloud vendors will offer service level agreements (SLA) to their commercial customers (e.g., AWS provide a 99.99% monthly uptime commitment in any given region). However, such services are provided on "commercially reasonable efforts", with exceedance of the SLA (i.e. failure to meet the service commitment) resulting in the issue of service credits.

When deploying applications to the cloud, one must design applications to be 'fault-tolerant', i.e. with the expectation that infrastructure components within the cloud will regularly fail, albeit that many such failures are managed within the infrastructure service and should not affect performance of correctly designed applications. Where applications require very high resilience, they will need to be deployed across multiple regions of the cloud platform - likely increasing the complexity of the application and its running costs.

Readers should note that free to use / sponsored services, such as those provided for sharing open data (e.g. AWS Public Dataset Program and Microsoft's AI for Earth), are typically not afforded any service level agreement at all. However, the infrastructure underpinning these services form a core of the cloud platforms and, as such, are highly unlikely to go off-line. Use of free offerings from cloud vendors will be very cost efficient, but should be assessed based on the risk to one's operations.

More fundamentally, public cloud vendors do not make long-term commitment on the provision of the infrastructure services themselves! However, given that cloud vendor's services provide a sustainable business, they are very unlikely to be discontinued unless a viable alternative is brought to market. Again, the only way to fully mitigate against this risk is to be prepared to migrate to an alternative service provider.

In the case of free / sponsored services, vendors will often commit for a fixed-term, with the ability to renew the agreement. For example, AWS Public Dataset Program commits to provide datasets on a 2-year term with indefinite renewal. AWS have never refused to renew a public dataset.

Finally, with reliance on third party services there will be a change in the skills and competencies needed by application providers (e.g. organizations hosting WIS Centres). It is likely that, in the medium to long-term, this will lead to gradual loss of in-house knowledge for skills and competencies that are no longer routinely used.

# Annex A - WIS 2.0 Future Technology Workshop Statement

In line with Resolution 23 (EC-70)[[8]](#footnote-9), WMO convened the "Future Technology Workshop" (19-21 March 2019, Geneva). Participants included experts from WMO, industry (Amazon Web Services, EUROCONTROL, Google, Inmarsat, Microsoft, Motorola, Thuraya, and Wisekey), and standards organizations: International Telecommunications Union (ITU), Open Geospatial Consortium (OGC), and World Wide Web Consortium (W3C). Representatives from private sector weather service providers were invited but unable to attend.

The workshop successfully achieved its aims, confirming that the concepts underlying [WIS 2.0 implementation approach](https://wis.wmo.int/file%3D4775) were aligned with industry directions.

***Challenges***

The technology industry recognized the challenges identified in the WIS 2.0 Strategy[[9]](#footnote-10). Increases in data volumes, demand for data usage, and the size, diversity and sophistication of audiences wishing to leverage those data are driving large-scale changes within the technology industry.

***Uncertainty***

All participating industry experts agreed that it would be impossible to predict with certainty how the technology industry and the services provided by the industry would evolve beyond 5-years. Only ITU speculated on the state of technology in 2030, identifying step changes that they expect industry to make. The Technical advances are often unexpected and rapid. Relevant macro-trends evident from the information provided included:

1. Rapid advances in provision and uptake of cloud computing services.
2. Massive increases in Internet bandwidth, connectivity and reliability.
3. Use Web services to expose data and functions in distributed systems.

***Reasonable Assumptions***

Based on the information from participating experts, some assumptions can be made:

1. The Web will continue to be the dominant distributed information system and will have managed backward compatibility as new Web technologies emerge.
2. Capacity and reliability of both terrestrial and satellite communications networks will significantly increase.
3. Hyper-scale vendors (Microsoft, Amazon Web Services, and Google etc.) will continue significant investment in public cloud platforms, and communities will coalesce around those approaches..
4. Technology vendors recognize that no one company can offer the complete solution. All vendors want to improve interoperability. Consequently, vendors will cooperate to provide complementary products and services, often using open standards to simplify integration.

***Confirmation of WIS 2.0 approach***

1. Technology industry participants concluded that WIS 2.0 is well aligned with current offerings from the technology industry and, in so far as is possible to assess, their future direction. For details, please refer to the Workshop report[[10]](#footnote-11).
2. Public cloud vendors (e.g. Amazon Web Services, Microsoft and Google) already deliver services with sustainable business models that appear to be consistent with the WIS 2.0 implementation approach. Furthermore, it is clear from the examples shared by the invited experts, that proven technologies can be used to implement WIS 2.0. Public cloud vendors recognise the need to interoperate with private cloud and on-premise solutions; i.e. hybrid-cloud. The Workshop outlines three risks for cloud-based operations and their associated mitigations. Public cloud vendors also highlighted the integration of artificial intelligence (AI) tooling within their platforms, thereby enabling their customers to transform the way they work with big data and driving cost efficiencies and/or new business opportunities for them.
3. GISC representatives noted that the Copernicus Data and Information Access Service (DIAS) and Climate Data Store (CDS) solutions adopted key elements of the WIS 2.0 implementation approach.
4. The aviation industry’s System Wide Information Management (SWIM) platform will support improved decision-making among and better collaboration between the many actors involved in Air Traffic Management (ATM). With sharing of authoritative digital information and data among a distributed community and use of Web services at its core, SWIM is a strikingly similar concept to WIS, albeit that SWIM includes ATM applications that consume data and information, whereas WIS stops with the provision of data and information itself. The WIS 2.0 implementation approach is consistent with the core principles of SWIM as presented by EUROCONTROL, and will drive implementation of a similar technical infrastructure approach. SWIM includes elements which ensure that services and components within the platform can be trusted. WIS 2.0 will also need to examine the concept of trust (verifiable identity, attribution, integrity and traceability of data etc.) in its design stage as has been done with SWIM.
5. WIS 2.0 will prioritise use of public telecommunications networks (i.e. the Internet). Participants agreed that Internet connectivity, capacity and reliability would improve markedly in the coming years. 5G will provide enhanced mobile broadband with gigabit per second (Gbps), ultra-reliable, low-latency communications. Meanwhile, satellite communication (satcom) networks expect a tenfold increase in capacity (with proportional reduction in unit cost), sufficient to allow users to interact with remote services and applications such as those deployed on cloud platforms and visualize derived products. Increasingly, network providers offer hybrid solutions combining both terrestrial and satellite-based communications. In short, industry predict that reliable Internet is coming almost everywhere at an affordable cost.

***Future considerations***

*Opportunities*

Following dialogue during the workshop, WMO and the World Wide Web Consortium (W3C) are seeking to establish a formal liaison similar to that already in place with the Open Geospatial Consortium. This will help to ensure continued alignment of WMO technical infrastructure policies, including those related to WIS 2.0, with the industry supported open standards that underpin the Web.

*Risks*

The invited experts identified cybersecurity as a significant concern, mirroring both the WIS 2.0 Strategy and the CBS-led review on emerging data issues in this regard. Given the broad reaching nature of implications, cybersecurity will continue to be addressed as a priority of Technical Commissions concerned with infrastructure and services. Activities will include a major refresh of the Guide to Information Technology Security ([WMO-No. 1115](https://library.wmo.int/index.php?lvl=notice_display&id=15901)).

The GTS ensures reliable delivery of mission-critical data to all NMHS worldwide. If increases in Internet capacity, reliability and coverage do not materialize as predicted by industry, then WIS 2.0 will be compromised. It is essential that WMO continue to monitor improvements in Internet capability and support Members in pursuit of UN Sustainable Development Goal 9[[11]](#footnote-12).

***Implementation***

Given the lack of long-term prediction from technology industry, workshop participants concluded that WIS 2.0 must be designed such that it is adaptable to change, thereby avoiding large cyclic investments needed to respond to technology change. It will be important to avoid over-prescriptive specification of technical standards.

The implementation of WIS 2.0 will introduce many new technologies to organizations participating in WIS. It is crucial to understand how to support the effective use of these technologies among those organizations. This will be achieved through the following:

1. WIS 2.0 demonstrator projects will show how these technologies can be used, and help the Regional Associations (RAs) and WMO secretariat clearly communicate the vison of WIS 2.0.
2. The WIS 2.0 implementation programme will work closely with the RAs and WMO’s Education and Training department to help develop and support effective training for NMHS to develop the competencies required for effective use of the technologies. With adoption of industry-standard approaches within WIS 2.0, NMHS will also benefit from availability of industry-provided training resources.
3. Information to be provided to Members to aid their considerations around using managed services supplied by the private sector or peer organizations, relying on partnerships rather than trying to build everything themselves.

It is important to note that WIS 2.0 does not require use of cloud platforms when implementing a WIS centre. Those designing the applications for a WIS centre will need to assess whether deploying applications to a cloud platform is appropriate. For more details on why one may choose to use cloud, please refer to the Workshop report.

Finally, participants recognised that changes to NMHSs’ mission-critical systems (e.g. the GTS; WIS 2.0 will introduce new protocols and phase out of GTS Headers) would need extremely careful management including an agreed transition period to avoid any disruption to safety-critical public weather services.

***Conclusion***

Information provided by partners and industry strongly supported the principles and core strategies described in the WIS 2.0 implementation approach.

The workshop confirmed that, to effectively respond to the needs of the WMO community, WIS will require the adoption of technologies unfamiliar to Members. It also highlighted the importance of evolving WIS toward an agile system that is able to respond to technology industry changes. A service-centric approach was promoted as the most effective mechanism to insulate WIS and its users from changes to underlying technology and systems.

Given continued investment from the technology industry in telecommunications, cloud platforms, artificial intelligence and more, the successful implementation of WIS 2.0 will depend on Members’ ability to leverage industry-supplied products and services – both free to use and paid for. To this end, WIS 2.0 must prioritize an ongoing commitment to training and capacity building among Members in all Regions.

-----------------------------------

1. Workshop meeting page [https://wis.wmo.int/page=eWIS-FutureTech](https://wis.wmo.int/page%3DeWIS-FutureTech) [↑](#footnote-ref-2)
2. WIS 2.0 strategy and implementation approach [https://wis.wmo.int/file=4865](https://wis.wmo.int/file%3D4865) [↑](#footnote-ref-3)
3. Workshop work plan [https://wis.wmo.int/file=5413](https://wis.wmo.int/file%3D5413) [↑](#footnote-ref-4)
4. Smallsat - <https://www.nasa.gov/content/what-are-smallsats-and-cubesats> [↑](#footnote-ref-5)
5. W3C study of practices and tooling for Web data standardisation <https://www.w3.org/2017/12/odi-study/> [↑](#footnote-ref-6)
6. Application Programming Interface (API): a clearly defined set of methods by which software components can interact [↑](#footnote-ref-7)
7. <https://aws.amazon.com/snowball/> [↑](#footnote-ref-8)
8. Resolution 23 (EC-70) <https://library.wmo.int/doc_num.php?explnum_id=4981> [↑](#footnote-ref-9)
9. [WMO Information System 2.0 Strategy (WMO-No. 1213)](https://library.wmo.int/s.php?h=e4359e95d0580936d608c9e20ac2a090) [↑](#footnote-ref-10)
10. Future Technology Workshop report [http://wis.wmo.int/file=5459](http://wis.wmo.int/file%3D5459) [↑](#footnote-ref-11)
11. Sustainable Development Goal 9: Build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation <https://sustainabledevelopment.un.org/sdg9>

Target 9.C: Significantly increase access to information and communications technology and strive to provide universal and affordable access to the Internet in least developed countries by 2020. [↑](#footnote-ref-12)