Quality Assurance and User Experience on Remote and Virtual Access

Expert Group I Report

November 30, 2023

Authors:

Hannele Savela, UOULU

Vanessa Spadetto, INTERACT-INPA

Expert Group members

INPA INTER⇄ACT

eRImote

Table of Contents

Executive Summary

The Expert Group I on Quality Assurance and User Experience on Remote and Virtual Access was created within the framework of the EU-funded project eRImote (*European Research Infrastructures - Pathway to Improved Resilience through Digital and Remote Access*) with the purpose of collecting experiences from both Remote Access providers and users on Remote Access provision to ensure the best possible quality of remote services.

Experts shared best practices and challenges in the Quality Assurance for Remote and Virtual Access. Defining a Quality Assurance Program with control steps is crucial to ensure the quality of the service, as it allows access coordinators to keep track of the process and detect problems quickly. Certifications can also help with this regard, offering infrastructures support defining quality guidelines and the quality review process. In general, infrastructure experts agreed on the use of a project management system as a good practice to facilitate quality access management.

Various softwares are employed in the provision of Remote Access, and some of them play an important role in tracking the access process, e.g. electronic logbooks and sample tracking and declaration systems. Other softwares improve the overall experience of Remote Access users, allowing them to remotely control the instrumentation, for instance. However, it was highlighted that the employment of softwares to open up the access provision chain to remote users pose an increasing risk of cyber attacks to the RIs, which need to pay more attention to cybersecurity measures, e.g. multi-factor authentication, segmentation of workflows, etc.

A second major challenge in Quality Assurance is sample shipping, which is not under RIs' responsibility, but nevertheless hugely affects the outcomes and quality of the access. Infrastructure experts underlined the need for an European framework for sample shipments, and shared best practices that partially overcome the issue, e.g. bilateral agreements with a single courier company.

Virtual Access poses different challenges in terms of Quality Assurance. Experts agreed that complying with FAIR data guidelines is the biggest challenge for the infrastructures, and enlisted good practices to enhance the quality of Virtual Access provision, such as the implementation of persistent identifiers and the definition of a clear Data Management Plan. Experts also noticed that infrastructures share the same obstacles in collecting feedback and statistics to review the quality of Virtual Access. GDPR regulations and the absence of any kind of application process to obtain the data restrain RIs from getting information on users and their experiences. Several possible solutions were discussed, such as the creation of user accounts and IP address harvesting.

Overall, several common challenges in Quality Assurance emerged during the discussion of the Expert Group among diverse infrastructures and across various domains, but also more specific difficulties related to the scientific field, e.g. protection of sensitive data. Valid solutions and successful best practices were shared, which were inspirational to the participants and that may be implemented by other infrastructures, manifesting the benefit and importance of establishing communication channels among RIs and across domains.

Introduction

The Expert Group I on Quality Assurance and User Experience in Remote and Virtual Access was one of the five Expert Groups established by the eRImote project consortium, to focus on Quality Assurance along the access provision chain of Remote and Virtual Access services.

The Expert Group aimed to identify current challenges and successful solutions in the Quality Assurance of Remote and Virtual Access services, as experienced both by the access providers and the researchers using the services. The Expert group thus intended to include the perspectives of European research infrastructures and the users of their services across different domains, service categories and geographical regions. The Expert Group I was led by INTERACT Non-Profit Association (from now on INTERACT-INPA).

In this report, Quality Assurance stands for the systematic process established to ensure the high quality of the service, in this case the Remote and Virtual Access to RI. Quality Assurance covers the whole chain of access provision, including the processes for user selection and guidance, training of staff, methods and platforms used in access provision, sample handling and sharing of results, and the collection and analysis of user feedback on remote and virtual/digital access services to RIs.

Quality Assurance can be explored through two different perspectives; as Quality Assurance simply looking at the quality of the data obtained through the access (reproducibility, accuracy, precision), or Quality Assurance as the quality of the management systems that make sure that the service process enables the collection of quality data (sample handling, data acquisition, data processing, data analysis, data transfer and storage, data retrieval). The Expert Group focused on the latter aspect, as the data quality standards and guidelines vary enormously from domain to domain, field to field, method to method, and are strongly dependent from the user’s applied methodology and practices.

The Expert Group discussed the most relevant topics concerning the provision of Remote and Virtual Access, focusing on the challenges and best practices adopted in each step of the process, from the application process for Remote Access to the reporting and feedback collection. Using the access provision chain as a backbone structure in discussions was helpful in ensuring that all topics were touched upon and helped to keep discussion structured.

Concerning Remote Access, sample shipping, safety evaluation and cybersecurity concerns were among the most challenging aspects in ensuring quality of the services, while for Virtual Access, complying to FAIR guidelines and collecting information on the data usage and attribution were found by far the hardest tasks from the quality management perspective.

Methodology

The experts participating in the group were identified through various channels: 1. The eRImote consortium partners suggested a number of experts to the Expert Group; 2. A registration form for expressions of interest in joining the group was distributed through websites, mailing lists and other communication channels; 3. INTERACT-INPA identified a few additional experts with the purpose of filling the gaps detected in the Expert Group outcomes, e.g. missing infrastructure domains.

The group was composed of research infrastructure project managers, access coordinators, data managers, technical staff, and researchers who have used Remote Access.

The work of the Expert Group was organised as on-line meetings. Altogether four meetings were arranged between March and December 2023.
In the first meeting, experts gave short presentations to demonstrate the best practices and challenges concerning Quality Assurance in Remote and Virtual Access provision at their infrastructures, whereasthe RA users described their experience with Remote and Virtual Access. The presentations were followed by a discussion on the topic best practices and challenges.
In the second meeting, the group focused on the main points of discussion detected in the first meeting and also on those not yet explored, such as protocols and guidelines, user feedback, sample shipping, and secure user authentication. One more expert presented their infrastructure RA/VA Quality Assurance structures and practices.
In the third meeting, results compiled from the previous meetings were revised to draft possible guidelines to be available for the public, e.g. other research infrastructures interested in improving their RA/VA Quality Assurance programs. One expert representing RI technical staff presented the Guacamole Apache tool for remote instrument control and cybersecurity concerns connected to RA/VA.
The fourth and final meeting was dedicated to review this EG1 report for submission to eRImote WP3 leads and to the eRImote information platform.

There were 10-15 participants at each meeting. Infrastructure representatives and users were from the domains of environmental science, life science, health and medical science, and social science.

Results

Remote and Virtual Access were discussed separately, as the two modalities of access hold very different features, as defined below. The Quality Assurance in Remote Access provision was explored by segmenting the access provision into the typical steps that users and facility staff go through to complete the access. Following the access provision chain allowed capturing of all possible challenges within each step of the process. On the contrary to Remote Access, Virtual or Digital Access does not have a clear access provision chain since the access is generally free and open to anyone, without e.g. user selection process.

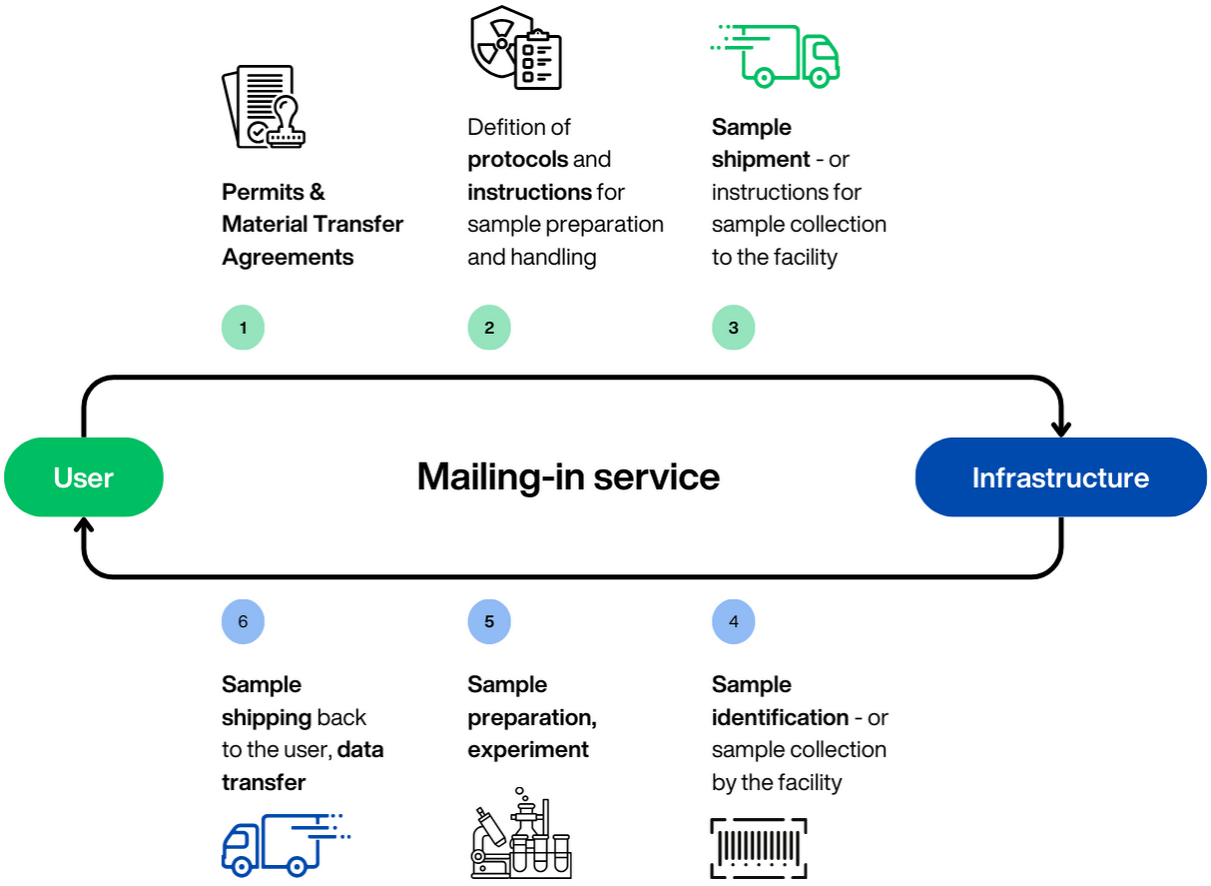
Therefore, the Quality Assurance in Virtual Access provision was analysed by first looking at the needs and challenges in providing data access to users, and secondly by the acquisition of results out of the access provided.

Modalities of access

Infrastructures have different conceptions of what is Remote Access and Virtual or Digital Access, therefore leading to different Quality Assurance measures and management practices.

Remote Access is defined as access to the infrastructure where the user is not physically visiting the infrastructure. Furthermore, different infrastructures may make a distinction between fully Remote Access and mailing-in Remote Access.

Mailing-in access consists of sending samples to be analysed by the RI for the users or, on the contrary, collection and shipment of samples by the RI to the users. In this case, the staff at the infrastructure has to complete the work that the user would have done if they had physically accessed the infrastructure, e.g. running the experiment and/or collecting data.



Fully Remote Access is a modality of access where the user is able to remotely access instrumentation located at the infrastructure to complete the tasks by themselves; the user might still send samples to the RI, but the experiment and data collection are done remotely

by the user. This modality of access requires specific softwares and authorization measures to allow the users to sign in and control the instruments through internet connection.

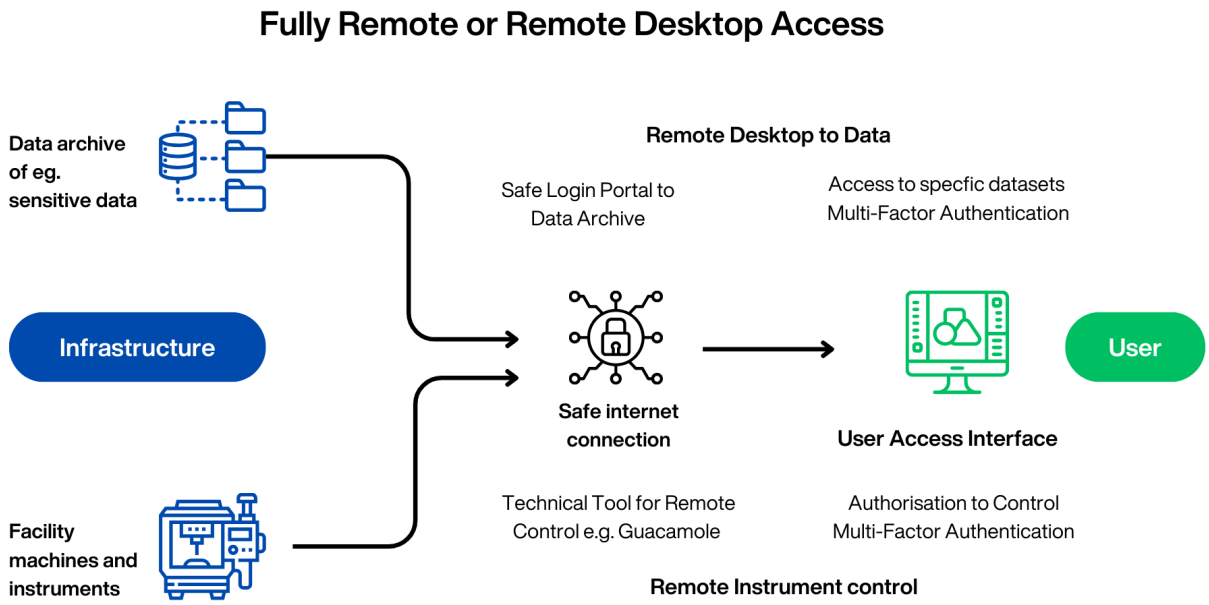
The choice on the utilisation of one modality or the other may depend on the type of experiments and users. Industrial users are generally employing the mailing-in service, while academic users are usually asked to access the RI fully remote, due to the more complex and various types of experiment they wish to carry on. On the other hand, in the biomedical domain, users may not be authorised to access the infrastructure at all due to hygienic protocols; mailing-in is therefore the only modality of access by default.

Nevertheless, not all infrastructures have the capacity to provide fully Remote Access or they might not find it preferable, and thus the user groups may need to utilise the mailing-in service or to employ hybrid access. In fact, ***hybrid access*** is another modality of access which entails both physical and Remote Access at the same time, with part of the group accessing the RI remotely and the other part being physically present at the infrastructure.

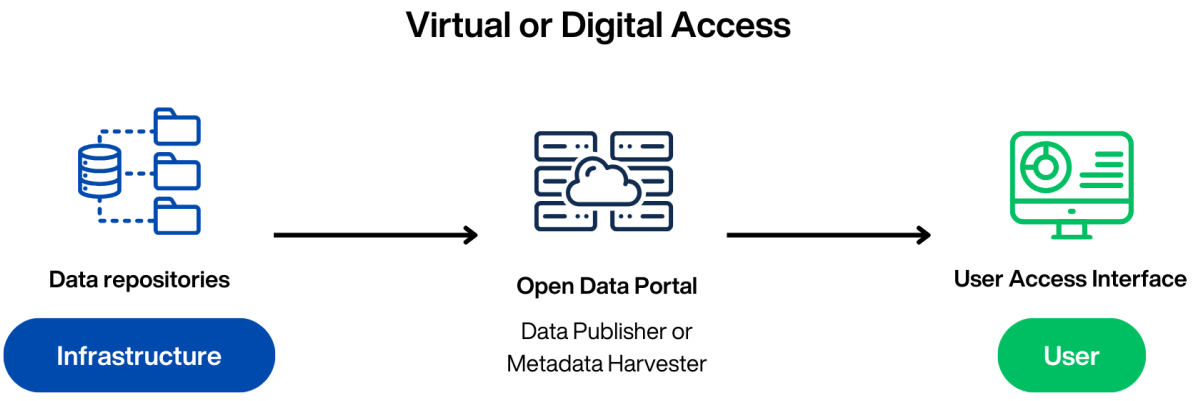
In the social science domain specifically, access is operated through **safe rooms**, where users cannot share or save any information, e.g. cannot upload or download any files in or out of the environment. Access through safe rooms is thus a modality of physical access that has been adapted to Remote Access in two modalities (Remote Access and Remote Desktop).

In both cases, the data are stored in the original repository and users can access them through a secure encrypted internet connection. In the Remote Access, users still need to physically access a safe room within the infrastructure, although they do not need to travel abroad, as they can go to a national infrastructure that has signed the agreement. This method is largely employed now and it is considered a safe way to provide Remote Access to users. To improve the opportunities for users to employ this modality of access, social science infrastructures in several countries have worked to build several safe access points across the country.

A more critical modality of Remote Access in social sciences is the use of Remote Desktop. Remote Desktop gives users access to sensitive data from a remote desktop that is outside the RI, e.g. user's institution office, through a login portal. Remote Desktop access is authorised through two-factor authentication which includes a biometric factor. Infrastructures then set up requirements to isolate and control the work environment, e.g. to be a private office with a fixed IP address. This modality of access is still not widespread as it involves a high risk of disclosure.



Digital or Virtual Access is a modality of access where the users are provided with data from the infrastructure. In most cases, the infrastructures provide free and open access to datasets containing raw or processed data collected by the infrastructure. In the environmental and natural sciences domains, this type of access is widely used. For other domains such as social sciences or health sciences where the data can be linked to individuals and often contains personal or sensitive information, open digital access is provided only to processed data that has undergone a consent, disclosure and security control. These procedures are essential to make sure that data cannot be manipulated or tracked back to identify people. Access can be provided to secured versions of the data (not anonymised) as a form of Remote Access, e.g. through project evaluation/approval, user identification, creation of a secure environment to access the data repository.



Quality Assurance in Remote Access Provision

A Quality Assurance Program for Remote Access covers the whole access provision chain. The experts identified several challenges and multiple new solutions at the different stages of the access provision process to ensure a high quality of the Remote Access service. In addition, the infrastructure representatives also came up with more general considerations on Remote Access as a modality of access itself, highlighting the opportunities related to it but also underlining several limitations of this type of access, as well as concerns associated with Remote Access, based on their experience.

General

Remote Access to RIs was very limited before the COVID-19 outbreak. As physical access was considerably compromised by the COVID-19 mobility restrictions, research infrastructures quickly reacted to the situation by shifting to Remote Access and enhancing their Remote Access capabilities.
With the decrease of pandemic cases and the possibility to travel again, physical access was restored as the main modality of access to research infrastructures, although Remote Access is still performed to a certain extent. Furthermore, Remote Access is considered beneficial in certain cases, as it allows wider user base to access the infrastructure (e.g. scientists from countries that have never accessed the RI before), it has a lower environmental impact and can partially decrease the costs of access (e.g. lower travel costs, but higher parcel shipping expenses).

However, Remote Access also has several critical points. For example, mailing-in overloads the RI staff with more work and responsibilities, whereas fully Remote Access exposes the RI to a high risk in terms of cybersecurity. Furthermore, staff at the RI are experts on the instruments and technology, but they may not necessarily possess the scientific knowledge required to properly handle samples, run the experiment and check the quality of the data obtained for the access user. In addition, the lack of in-person users at the RI affects the knowledge exchange between users and facility experts, decreasing hands-on training opportunities that are particularly important for the young scientists and lowering networking opportunities.

For this reason, the combination of Remote and Physical access (hybrid access) was considered very beneficial to the research infrastructures, as it allows sufficient number of user group members to visit the infrastructure via physical access to successfully conduct the study, while giving an opportunity to the rest of the group to follow the work remotely, thus lowering the carbon footprint and travel costs of access.

On the other hand, fully Remote Access works well for simple experiments with a high level of automation and standard and straightforward instructions and procedures, therefore implying minimal sample preparation and null or minor safety considerations for sample handling. In fact, safety evaluation is a considerable issue for Remote Access. While RI staff may not know how to correctly handle the samples especially if the instructions from the users are not properly clear, for some types of experiments the users may not be sufficiently

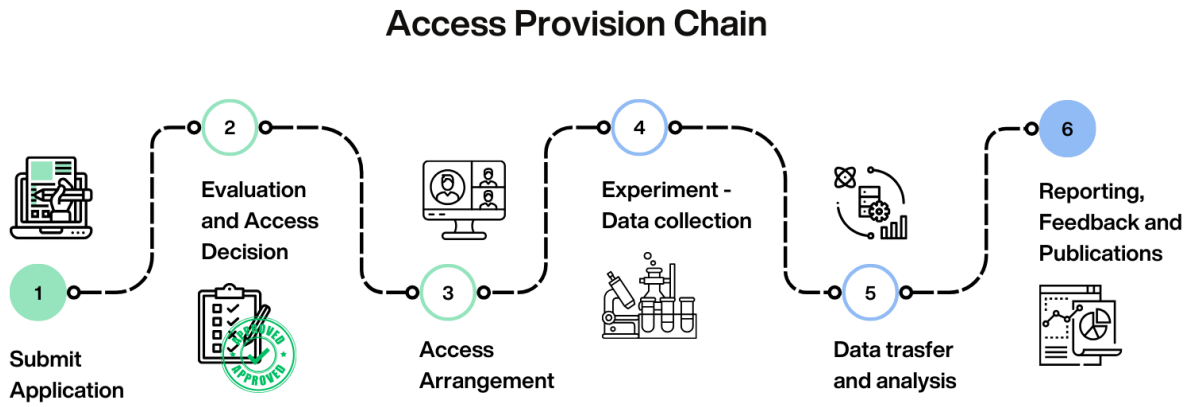
qualified to run the experiment by themselves remotely, especially due to security concerns, and would thus need to come on site and be supported by the local staff.

Overall, the expert group members agreed that the emergency solutions regarding RA provision that were developed to respond to the pandemic crisis are not sustainable in the long run, especially regarding mailing-in services due to the amount of workload and responsibility they pose on the RI personnel. The solutions taken to provide full Remote Access -on the other hand- present different kinds of concerns, first of all the risk of cyber attacks and the danger connected to exposing the RI core activities and instruments on the web.

Quality aspects along the Access Provision Chain in Remote Access

Remote Access to RIs is generally operated through open calls, which can be continuous or periodical. In general, infrastructures seem to adopt a similar framework for their access provision chains, which is usually a modified version of the physical access provision chain.

The access provision chain usually begins with the call proposal. Once the proposal is submitted, it is then reviewed and evaluated by evaluators assigned by the infrastructure management team. Infrastructures can set different standards to evaluate the proposals, although the evaluation generally includes scientific, technical and logistical evaluation. If the proposal is approved, the access is arranged with the infrastructure personnel or the possibility to access instrumentation remotely is provided to the user. Once the samples or data are collected, they are shipped or transferred to the users, who can analyse them; the RI may also provide softwares to analyse data in a defined environment. The access ends with the data or sample analysis. The data analysis produces results which are usually published through journal articles or scientific publications. At the end of the access provision chain users can be requested to provide a project report and/or provide costs and access details; in addition, infrastructure may ask users to provide feedback on the service and to acknowledge the infrastructure and/or the grant agreement in any publication resulting from the offered access.



Remote Access differs from physical access mainly by the access arrangements, sample or data collection and analysis. However, these changes consequently affect the whole access

provision chain, as different or additional measures need to be taken into account throughout the whole process.

Shifting to Remote Access implies the need for a higher amount of information exchange and requirements to satisfy in order to offset the imbalance generated by the lack of physical access to infrastructure and therefore of in-person security check and exchange between users and staff. In the case of remote instrument control or Remote Access to secure data, the user must comply with higher security requirements (e.g. multi-factor authorisation) as these modalities of access notably increase the risk for the infrastructure, e.g. exposure of core activities or sensitive data to external users.

Quality Assurance Programs and Quality Certificates for Access Management

Designing a Quality Assurance program for Remote Access requires identifying the specific features of Remote Access that differ from the physical access, the challenges that they raise and evaluating possible solutions.

Eventually, Remote Access management is in most cases a fraction of the overall access management, which is still largely composed of physical access. The infrastructure management may take advantage of an overarching quality management certification to tackle the challenges in offering high quality services, support and access outcomes. Several infrastructure experts mentioned ISO 9001 certification as a good practice in quality management, as the ISO protocol is needed to acquire the highest quality data. The 5 Safes framework instead is a summary guidance scheme widely spread within the social science domain to guide infrastructures to ensure safe access and non-disclosure to sensitive/personal data. In general, it is recommended to implement quality control steps and parameters such as KPIs (Key Parameters Indicators) to easily recognise any anomaly in the access provision and to monitor the quality level of the access management over time.

ISO Certificates and Guidelines Examples

The ISO 9001 Certification was the most common certification protocol brought up by the infrastructure experts.
The ISO 9001 Certification requires RIs to follow standards and guidelines which apply to different stages of the access provision; the certification provider offers guidance on setting up the RI Quality Assurance guidelines and measures and does not impose pre-made guidelines, but may suggest already existing guidelines if they are widely recognised Quality Assurance guidelines for the specific domain in question.
One of the requirements of ISO 9001 is to follow and harvest all problems and malfunctions that can help to improve the instructions provided to the users. Ri staff can use a technical tool or software to harvest all the problems occurring

during the access (including issues with communication). This can be a good practice to improve protocols and to make communication easier.
In addition, certifications can be a requirement by industrial users for disclosure agreement and Quality Assurance. On the other hand, academic users are usually not so interested in quality management certifications, and they look more at the quality of data. However, certifications serve also as a branding point for the service providers. Service providers that have quality certifications can score higher in public tenders, and can also use the certification to boost their reputation as a guarantee of their services.

Designing a Quality Assurance Program

Different approaches can be taken to design a Quality Assurance program.
As an example of a bottom-up approach, one infrastructure represented in the Expert Group designed its Quality Assurance Program by asking each facility what kind of services they can offer, what is needed to perform such services, what they use and what is the outcome to the user. For each of these steps, the facility managers were asked to list the most critical points to ensure the quality of the service. Where a high level of risk to quality was detected, the RI defined some control measures to ensure that the level of criticality was covered.
As a more top-down approach, one infrastructure designed its Quality Assurance Program on a three-layer approach, having Key Quality Principles as the first layer, Common Standards e.g. shared or harmonised SOPs as the second layer, and local and national regulations, e.g. specific or national SOPs as the third layer. The Quality Principles are used for self-assessment of quality at the facilities and to exchange best practices.
Infrastructure experts underlined the importance of implementing KPIs to assess the quality of the access provision. For instance, one interesting KPI is the duration of access from the access proposal to the reporting stage. Through this parameter, it is possible to detect stages or operations that are more challenging to complete, and if any project or facility is particularly delayed. Other possible KPIs can be introduced, for example, in the evaluation stage, by identifying a threshold in the evaluation scores for scientific excellence.

Call and application stage

The first stages of access provision do not substantially differ between remote and physical access. Infrastructure experts noted that the call description and application guidelines for Remote Access need to be more detailed in regard to e.g. what the infrastructure can provide to users, while the users should be requested to be clear and specific on their needs, objectives, and methods, as well as on the required conditions of the samples, price and duration of the experiment. These specifications are needed to properly evaluate the technical and logistical feasibility of the research proposal.

Social science research infrastructure dealing with personal information may require specifications on how the data will be used, what data specifically, who will access it and for how long, with a specific motivation behind the request for secure data. Therefore, the evaluation will also take into consideration the disclosure risk and the proposal process requires applicants to provide specific information to be included in a Data Use Agreement.

Support to access applicants

Some infrastructures, especially when offering access through periodical calls, offer support to applicants by providing information on the application procedures through webinars and by email, including scheduling Q&A sessions with applicants. Other, more indirect forms of assistance have been developed too, for example matrices and tools to guide applicants to choose the best modality of access and the most appropriate facility where to conduct their research. This type of support helps the users to evaluate before submitting their proposal which modality of access -be it remote, physical or virtual- would be the most feasible for their study.

Evaluation and Access Decision

The evaluation process can have different standards and procedures depending on the domain, infrastructure type, grant framework, etc. Generally, the evaluation process involves a technical, logistical and scientific excellence evaluation; it can also include, among others, an evaluation of users' background and a consideration of cost-efficiency. Other more specific criteria can be implemented, as in the biomedical or social science domain, where ethical considerations are also taken into account when dealing with live animals, or people.

Unlike physical access, Remote Access projects usually require increased work for the RI staff. Although remote and physical access proposals are generally evaluated according to same standards, evaluators should take into account the feasibility of the study in terms of workload for the facility staff, the level of automation, and give particular attention to safety evaluation, e.g if the staff is trained and knowledgeable on the type of sample in question and the related sample handling procedures. Therefore, time and effort are relevant criteria in the evaluation of Remote Access projects.

Project Management systems

Although it is not specific to Remote Access, it is noticeable that many infrastructures have developed or adopted a project management system for users to be informed on open calls and apply for access. The same software can also be employed in the later stages of the access provision chain, e.g. proposal evaluation, access decision, reporting of activities, in some cases also for the collection of user feedback and resulting publications. Such a system allows the infrastructure to be considerably more organised and efficient, and to store and harmonise information across projects and users. A project management system thus strongly improves the quality management of access provision.

Access arrangements

The access arrangements vary from infrastructure to infrastructure and among single facilities too, considering that distributed infrastructure often includes facilities from different countries. In fact, distributed research infrastructure may have difficulties in setting up standard procedures as the single facilities are so different and operate according to their own regulations.

Protocols

For infrastructures dealing with samples, the access arrangements include the definition of protocols for the sample preparation and handling, in addition to description of sample content and related risk assessment (hazardous, toxic, carcinogenic or infectious material, for instance). The facility should also know in detail the degree of decision making and responsibility given to the facility staff when running the experiment or collecting data.

To set up such protocols, infrastructure often has to schedule calls between the facility staff and users. In fact, infrastructure users participating in the Expert Group particularly underlined the importance of a fluent communication with the facility managers to define the protocols, especially to see how such protocols needed to be adapted to the facility capabilities and available instruments.

Infrastructure experts also highlighted the use of several control steps or points within the protocols and in the lab books or work logs to ensure traceability as a best practice. Many infrastructures do not have general protocol templates for users. However, some infrastructures have developed an experiment protocol template to help users navigate the Remote Access. The experiment protocol was described by experts as one of the most difficult steps in the access provision chain during the emergency response to COVID-19 situation. Other infrastructure preferred to focus on direct communication, and invested a substantial amount of time in calls and meetings with users to define the protocols.

Considering the large variety of services and techniques that the infrastructures can offer, it is very difficult to come up with a standard experiment protocol; the infrastructure would need to create one experiment protocol for each group of instruments or techniques. Moreover, infrastructures should also evaluate the most efficient way to proceed according to the scale and type of services provided; in fact, for infrastructure offering often only a limited amount of Remote Access or dealing with very diversified types of experiments, more

straightforward types of communication, e.g. email exchanges, are easier and more practical than standardised protocols.

Agreements and permits

Access arrangements can also include signing agreements between RIs and users or their institutions. Besides general agreements on the granted access to the user, other types of contracts may be necessary.

In the social science domain, the agreement between the users and the data service also include binding and legal terms, conditions and restrictions on the use of provided secure data, e.g. Data Use Agreement. Agreements can also be signed for sample shipping or any kind of material transfer, especially when dealing with biological or patented material, e.g. Material Transfer Agreement. It was noted that MTA can delay the access schedule as they involve parties that are not under RIs control. Other disclaimer and disclosure agreements between parties may also be requested, especially by industrial users.

In addition, when preparing for Remote Access the users should also be directed to application procedures for any necessary or mandatory permits to conduct their research at the infrastructure, e.g. national permits for sample collection and transport.

Training

Moreover, access arrangements should include the necessary training. Training is an important step to ensure quality of Remote Access, as it lowers the possibilities of mistakes during the process by filling gaps in knowledge at different steps. For instance, remote instrument control is particularly challenging, and therefore some infrastructures have prepared video training lectures or scheduled webinars with the applicants to demonstrate concretely how to proceed. In the biomedical domain, training modules have been developed to enable users to prepare and handle samples shipped in frozen conditions, so as to diminish the need for transporting living animals. In the social science domain, it has been noted that users may not understand the requirements for working with secure data. Some infrastructures have imposed training modules as a mandatory requirement preceding the use of the granted access.

Also the facility staff may benefit from training Remote Access deprives facility staff with the opportunity to directly learn from the researchers coming physically to the infrastructure to conduct their experiments, and infrastructures have noted the increasing challenge of having facility staff that is knowledgeable both on the scientific and technical aspects of experiments, both of which are needed to conduct the Remote Access for the users.

Multi-Factor Authentication

Finally, since fully Remote Access entails a higher level of security risk in terms of cyber attacks, users must also comply with the guidelines and requirements for safe access, e.g. multi-factor authorisation, identifiable personal account, no password sharing or one-time passwords, strong password settings etc. Several infrastructures have introduced **multi-factor authentication** and consider it a minimum requirement to improve the cybersecurity of the infrastructure’s systems. Multi-factor authentication is a multi-step

account login process that besides email and password asks for other information in order to sign in, usually an OTP (one-time password). OTP functions for a limited time and requires a separate device or contact point, making it more difficult for different users to access the same account.

An additional step can be to implement Single Sign On, meaning that the user needs to create only one set up to log in to all of the infrastructure's services. This authentication solution improves the user experience by making it more straightforward. However, in this case the infrastructure must pay extreme care in terms of updates and potential cyber attacks, as one attack can harm several systems at once.

Data or sample collection, handling and/or processing

Quality in access provision is best ensured when actions related to access provision are tracked and registered, so that it is possible to identify issues and isolate them from non-problematic actions.

Sample tracking and declaration

Infrastructures specifically underlined the importance of declaring and tracking samples correctly, and to assign ID to samples with e.g. date of receipt, storage and return conditions for that. This process can be automated through software, as many infrastructures are already doing. Also, the control and maintenance of instruments can be done through log books, and calibration records help to obtain more FAIR and standardised data.

Sample handling procedures

Guidelines on sample preparation and handling are usually not generic but instead often highly specific to each domain and technique/method. Some domains may not have shared guidelines at all, whereas some domains may have more standard procedures since the samples are more sensitive (e.g. health data) or easily deteriorate over time (e.g. biochemical compounds), thus requiring very precise handling. Quality Certifications may help with this step, as they may direct the infrastructure to existing shared guidelines or help them set up standard guidelines where they are not available.

Depending on the modality of Remote Access, the data collection procedures vary. In the mailing-in service, facility staff commits to following the established protocols, fills log books to keep track of each step of the experiment and is usually in contact with the users through various communication channels, depending on the infrastructure. Some infrastructures give the possibility to exchange messages between the staff and the users via the log books or project management softwares, others do so by email.

Remote desktop access and instrument control

In the fully Remote Access modality, users are able to remotely control the instruments and conduct the experiment without the support of the staff, even though they still usually stay or re-visit the instrument room to do regular check-ups. In the physics domain, for example, several infrastructures have introduced Remote Desktop access thanks to a technical tool that records what is happening inside and outside of the instruments. The open source

version of such a tool is called **Guacamole Apache**, and also other commercial solutions exist. The tool allows the infrastructure to give authorization to users for remote control of the instrumentation, for duration and time defined by the facility and synchronised with e.g. the beamline planning control mode is therefore also dependent on the level of automation of the instrument itself.

Use of Guacamole Apache was appealing to the infrastructures that wished to quickly react to the pandemic and start offering Remote Access. Despite the satisfying rates of security that Guacamole Apache offers, it is important to note that such solutions expose the infrastructure to a high risk of cyber attacks.

Remote desktop access through Guacamole Apache or analogous tools is nevertheless often and best used in hybrid access form, with one or two scientists coming on site and the others following remotely.

Guacamole Apache: an Open Source tool for Remote Desktop Access

Guacamole Apache is a technical tool used during the experiment session, data processing and data transfer that allows users to remotely access the instruments located at RI. .
Guacamole Apache setup comes together with a video conferencing system in the instrument cabin, so that the users are able to see what the machine is doing, both from the inside and the outside. The set up can be adjusted to adapt to the needs of the users or specifications of the machine.
To obtain the control of the machine, users must be authorised by the staff. Authorisation reply can also be automatic. Users can have either read-only access or full control over the machine. The full control option is not preferred and should be employed only when the staff is not available, e.g. night time. Nevertheless, even in the full control mode, the staff still retains access to the instruments and can support the users if needed.
Guacamole Apache provides a remote computer display, a system to manage access rights, has a relative fine grain resolution, and allows both session sharing and session recording. It also includes a help-desk centre contact for users, which generates a trouble ticket for each support request.
The system can easily be integrated with other softwares, e.g. the user portal, through ETL. This allows Guacamole Apache to automatically insert and register the new planned experiments according to the information in the RI project management system.
Guacamole Apache is also well managed concerning cybersecurity; it detects weaknesses and announces them so that the staff can quickly react, and it

gives protection also with regards to RDP VNC protocols, which are quite vulnerable to cyber attacks.
Setting up Guacamole is relatively easy and cheap, and it's a general purpose solution. Guacamole Apache needs a certain bandwidth to operate, and there have been. An infrastructure has witnessed initial issues when users have not been able to couldn't reach the minimum bandwidth length. This can be resolved by the infrastructure by setting a small system for users to check their bandwidth and imposing the minimum bandwidth length as a prerequisite for remote instrument control.
The security risk in adopting an external instrument control system is still very high despite the various security measures, and infrastructure should work on developing an ad hoc system for these purposes, exposing only the minimum information and control options on the web..

Sample shipment

Sample shipment was identified as one of the most prominent issues related to Quality Assurance within Remote Access provision. This is because sample shipment is associated with risk to the sample, as neither the RI nor the user has no control over the samples en route since they are usually transported by a third party courier company, and delays or adverse shipment conditions can often deteriorate the sample content to the point that is not anymore suitable for analysis.

It is also worth noting that different regulations and restrictions concerning sample content may apply depending on the samples sent (e.g. organic vs. in-organic samples), whilst some hazardous material cannot be shipped at all.

Need for an European sample shipping framework

Infrastructures participating in the Expert Group expressed the need for an international or at least European framework for sample shipments. As sample shipping is by volume and money a very small, and thus a rather irrelevant part of the business for the courier companies, the individual infrastructures have no leverage to ask for better or specific shipping conditions. Also the Brexit heavily impacted infrastructures' possibility to carry on Remote Access experiments, as shipments from/to the UK were blocked or delayed, for example the shipping of live animals.

Bilateral agreements, new technologies and courier recording

As a good practice to tackle the challenge of sample shipping, few infrastructures have signed bilateral agreements with a courier company on which they have chosen to rely on. Another very interesting solution was found by an infrastructure, which worked together with

shipping companies to develop a new technology that makes samples stand more simple and less demanding transport conditions, e.g. resist higher temperatures. Finally, another good example to follow consists of asking users who ship samples to specify in their post-access feedback which courier company they chose and how was their experience. By detecting common patterns in the feedback, it is possible to identify which companies better preserve the quality of the samples and use their services to ensure high quality in sample shipping.

Data transfer and analysis

Infrastructures have different softwares and ways to transfer the data to the users once the experiment is concluded. Once the data has been extracted from the machines, the data transfer to the user can be done through the institution's cloud services, a specific designed software or software the infrastructure adopted together with other RIs. The size of data may vary considerably depending on the experiment and domain, and some infrastructures have developed solutions to allow users to download experimental data of more than 50TB, e.g. Globus software.

Some of the data transfer systems allow the users to sign in, search for their results, for instance crystallisation images, and download them on their computer; other systems also allow users to process and analyse data with a software in defined environments, e.g. Virtual Infrastructure for Scientific Analysis, enabling users to remotely analyse data from facilities during or after the experiment. While for certain domains - like life and environmental sciences - a virtual safe environment is beneficial to the user but not requested, for the social science domain it is sometimes mandatory, due to the disclosure risk and the need to ensure that sensitive raw data are not downloaded on personal computers or shared with unauthorised people.

For infrastructures owned by a public institution e.g. university, a good practice to take example from is to create a separate VPN pool for the infrastructure's users on the university's cloud server, and then provide users with temporary accounts assigned to the specific VPN pool, which are also protected by Multi-Factor Authentication.

A specific challenge mentioned by Infrastructure experts was the temporary storage of data, i.e. data is stored by the infrastructure only a limited amount of time (depending on e.g. server capacity), which will then be deleted after a certain deadline. After that the data is only stored on the scientists' personal computers, making it difficult for the RI to track how the data is used, publications resulting from the data etc.

An important step in the prevention of losing track of the data produced at the RI, and to improve quality of data management in general would be the use of persistent identifiers, e.g. DOI, for experiments and/or datasets, which would allow tracking of experiments and data, and linking them with different software and the RI where the data was collected.

Reporting, Feedback and Outputs of Access

Reporting and feedback activities can be more or less developed among infrastructures. RIs that receive public funding through e.g. EU funding frameworks are committed to following specific requirements which entail detailed reporting of costs, use of access and research outcomes. Usually such infrastructures have some sort of reporting and feedback instruments in place to keep track of the outcomes of the granted access, although experts agreed that improvements could be made on the feedback questionnaires.

Feedback from users and facilities

Whether mandatory or not, users are often requested to give feedback on their experience with Remote Access. Nevertheless, the same feedback form used for physical access does not fit well with the experience of a remote user, who cannot provide comments on the quality of the physical infrastructure facilities, for instance. Whereas some infrastructures still use a joint feedback form for all users independent of the modality of access used, others have developed new ways to acquire feedback on Remote Access specifically. A good example comes from an infrastructure that uses a feedback questionnaire platform that allows different paths depending on the responses, e.g. if the users checks the box for Remote Access, the system will give them questions that concern Remote Access specifically, and vice versa for physical access. Questions can be very generic, e.g. asking whether Remote Access met their expectations with a possibility to a comment, or quite specific, like for instance, asking to upload the best images of results and conditions of sample preparation. The need to ask generic vs. specific questions also depends on the conducted experiments and adopted techniques at the infrastructure. If it is not possible to filter questions in the feedback form according to modality of access, it is then recommended to create a separate questionnaire for Remote Access. Feedback responses should be analysed periodically, with consequent actions, to make sure that the concerns and suggestions from users are feeding back into the Quality Assurance process.

Feedback from the facilities concerning access is also very important. While it is not common to ask feedback from infrastructure managers for every project granted access at the facility, periodical or ad hoc surveys are in several infrastructures circulated among the RI staff to obtain their feedback on the access provision. While there are no standard guidelines for this practice, various infrastructures are working on collecting challenges and best practices on their Remote Access services as experienced by their facility managers, e.g. LEAPS, NMR Remote, INTERACT, and this aspect is also widely surveyed across infrastructures and domains in eRemote.

Reporting Remote Access outcomes

Project reporting can include multiple kinds of information from the amount of access used and outcomes of the research conducted with access to declaring the costs associated with the access. Requirements for reporting depend on the funding scheme of the infrastructure, affecting the reporting further to the funding bodies. A robust project management system considerably helps in reporting the access associated costs and analysis of different statistics and key indicators from the project reports.

One of the key outcomes from access to RI, and an indicator measuring the success of access provision in many funding schemes, are the publications produced by the RI users. This makes the collection of publication records an important part of the reporting. In the social science domain it is furthermore very important, that the RI has a possibility to pre-check manuscripts and data outcomes resulting from the granted access before their publication to make sure that no sensitive data is shared.

There are several ways how infrastructures collect publication records, but unfortunately none of them are usually very effective; users may be requested to add their publications into the reporting system or a similar repository, they can be asked information periodically by mailing list, or the infrastructure may look for acknowledged publications by searching from portals and repositories with the grant agreement number. Furthermore, publications may be produced and published years after the access takes place, making it even more challenging to have users provide their publication records retrospectively.

Collection of publication records resulting from the granted access as widely and reliably as possible was found as a critical step in the reporting stage to demonstrate the scientific value and quality of access offered by the RI. The infrastructure experts agreed that the number of publications where the infrastructure use is currently acknowledged is very likely only a minor part of the actual amount of publications coming from the granted access. Combined with the modest success in collecting publication records from the users, it is more challenging for the RI to demonstrate excellence in research as an outcome from their access services. Again, introducing wider use of DOI and persistent identifiers for RI, experiments and data would help to relieve the situation.

User experience

User representatives of the expert group emphasised the benefits that Remote Access provided for their research. For example Remote Access allows researchers to conduct experiments across a larger environmental gradient than with physical access or hybrid Remote Access has allowed the expansion of the scientific aims and objectives of the research project to new and novel areas. These positive aspects contribute to the more usually mentioned benefits of Remote Access, e.g. lower carbon footprint.

As a downside, access users mentioned that Remote Access required a higher amount of communication with the RI to specify details of the experimental protocol and methodologies. Communication is essential to define protocols to obtain high quality and reliable data, and users had to often go back and forth with the facility staff to edit their protocols according to the capacities at the facility, which the users would not have known otherwise.

Cybersecurity

Cybersecurity was a low priority before the COVID pandemic, but now that RIs are exposing more of their network online the topic has become particularly relevant.
Fully Remote Access through remote instrument control is risky in terms of cybersecurity, independently of the software or tool that is implemented to offer the remote service. Data collection and analysis are the core activities and principal outcomes of the research infrastructures, and to expose the data production chain to external, remote users corresponds to providing access to the production network of a company. There are, however, measures to mitigate and partially offset the risks.
Network segmentation is one of the measures to lower the possibility of a successful cyber attack and mitigate the impacts of the cyber attack if it breaks through. Infrastructures should also make sure that users are well-identified by requiring user identification, removing generic accounts and utilising multi-factor authentication.
Finally, logs should be externalised and it is absolutely crucial to keep the security system and measures up to date.
Users should be informed about and required to follow cybersecurity procedures, since many frequent actions taken by users are responsible for lower cyber protection, e.g. setting weak passwords, changing passwords infrequently, and especially exchanging user credentials with others.
Cybersecurity is a real risk for infrastructures developing more and more services online; several facilities have already experienced successful criminal cyber attacks and have been forced to shut down their operations for extended periods of time.

While some infrastructures are interested in implementing remote instrument control tools such as Guacamole Apache, other RIs that are already employing such software warn that this should be a temporary solution and that RIs should focus on the development of *ad hoc* safer tools. Such software would expose only the control software through a web interface, but as this kind of system is set up from the beginning it thus requires a substantial amount of time and budget. As a best practice to pay more attention to cyber security risks and their mitigation, RI or domain-specific groups discussing cybersecurity issues and related risks and sharing solutions might prove valuable.

Software utilised along the access provision chain

Both remote and physical access provision often employ several softwares along the access provision chain. Infrastructures use project management softwares for access calls and proposal management, for the evaluation of proposals, to grant access and to report activities and costs at the end of the process. A comprehensive project management system allows the infrastructure to automatically report figures and costs on granted access, to derive statistics on users or research topics, but it also provides the access coordination and administration to monitor the status of different projects and react to any problems or issues fast and efficiently.

Several infrastructures have developed their own project management system to best adapt to their needs (e.g. ARIA system, INTERACCESS system), but commercial solutions are also available. In fact, some of the project management systems developed by the infrastructure have then been optimised to be offered on the market to other access programs, projects or infrastructures, e.g. ARIA. Infrastructures may use the same software also to collect feedback and communicate with the users, or have externalised those functionalities on another platform.

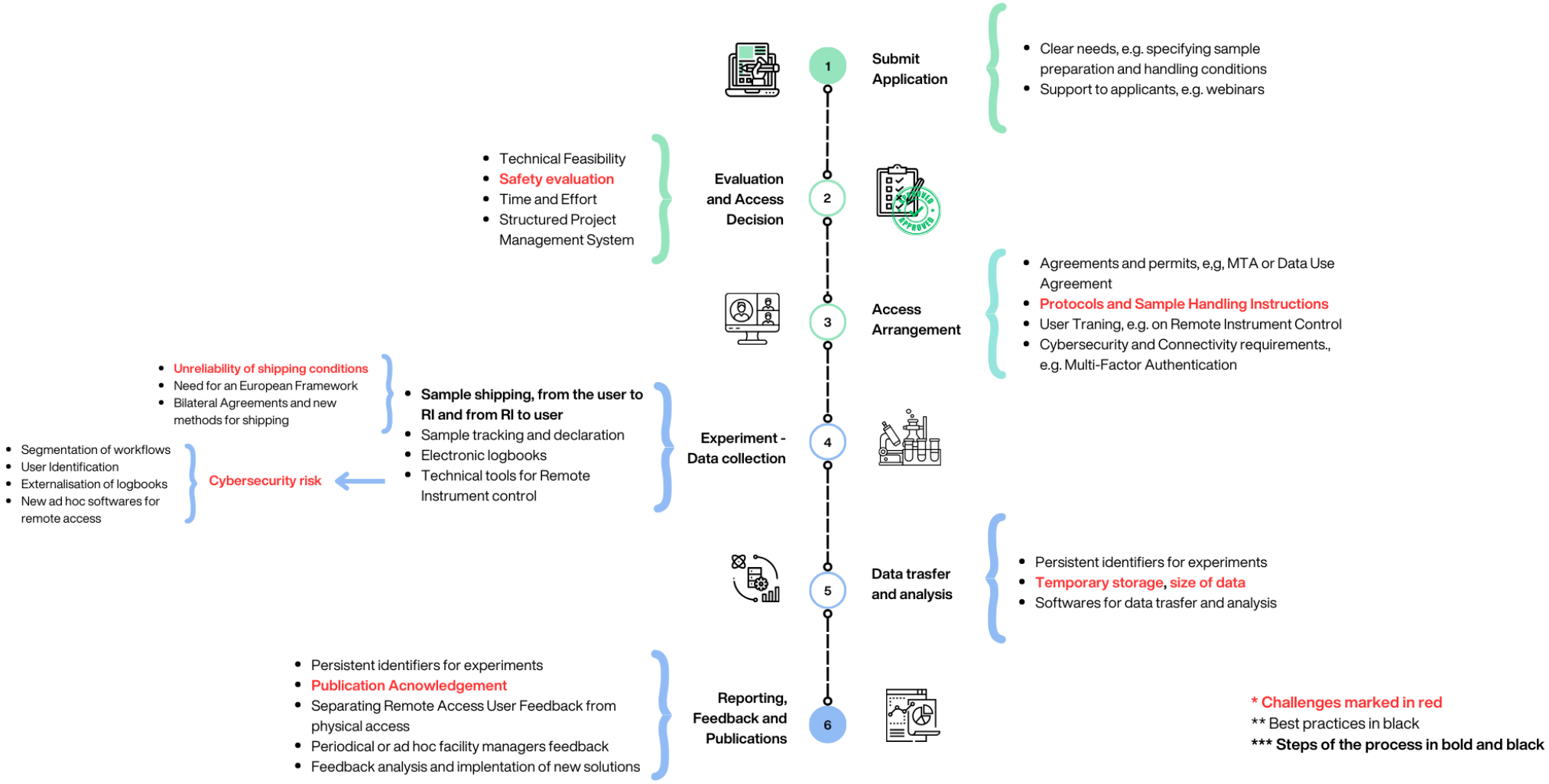
Other software are utilised for data transfer, especially when it involves data of large size, e.g. Globus. Sample tracking can also be operated automatically through an online system, such as electronic logbooks.Depending on the scientific domain, several infrastructures are also adopting systems to view, analyse and process data online.

Employment of electronic logbooks was underlined as a best practice by the infrastructure experts to ensure a better quality of data acquisition and experiment procedures.

Software development and maintenance require a large budget and a considerable amount of time. Before deciding to switch to another software, or develop custom software for their purposes, RIs should first check to make the best use of the softwares already in place, which may need only some additional features to be optimised.

Finally, the difficulty in hiring new software developers was identified as a critical challenge in this regard, as the professionals in this field are in high demand, and public institutions do not have possibilities in terms of resources to compete with the private sector e.g on the salary level.

Summary of Quality Assurance Challenges and Solutions in Remote Access



Quality Assurance in Virtual or Digital Access

Virtual or Digital Access is usually offered by the infrastructures as free access to datasets through open data repositories. As the access is open and free, this modality does not involve any application process, project proposal, access decision or other specific arrangements. Data can be accessed anytime, can be downloaded as many times as desired and can be stored and analysed anywhere. Most open access data repositories do not ask for formal requests, have no time limit for access and no user identification. The reason behind this is that the aim of Virtual Access is to keep data as open and accessible as possible. Virtual Access enables the reuse of existing data and thus avoids duplication of efforts and maximises the utilisation of data.

The access provision chain of Virtual Access largely differs from Remote Access, as it does not include several of the steps, e.g. access proposal, evaluation and data collection by the users. Instead, the actions to provide Virtual Access and challenges in the process can be divided in two larger sections: measures on data handling and management in order to give access to the data, and data access outputs and feedback once users have downloaded the data.

Data Handling, Management and Provision

Ideally, infrastructures should have a well thought plan for their data management from the data acquisition to the stage when data is published and offered through Virtual Access. A solid Data Management Plan is essential to ensure the quality of Virtual Access provision, since the data that is not collected according to standardised metadata and data formats, it will need much more further processing to comply with FAIR guidelines.

Challenges: FAIR Guidelines, GDPR and data handling

Complying with FAIR guidelines to ensure that data offered for Virtual Access are Findable, Accessible, Interoperable and Reusable was identified among the most challenging issues for infrastructures offering Virtual Access. Ideally, data should be standardised from the beginning, therefore infrastructures should have standard guidelines for data acquisition and utilise standardised equipment. That is extremely difficult to execute even within small national infrastructures, and even more challenging in wide multinational distributed infrastructure networks.
Distributed infrastructures offering Virtual Access also struggle with identifying common metadata standards that can be applied by all facilities within the network. Defining metadata guidelines for the infrastructure does not only entail agreeing on shared standards, which can sometimes be impossible, but also includes training and educating the facility staff on data management, metadata and data standards, as they do not necessarily have knowledge on the IT aspects of the data.
Data providers have to also to make sure that the data is compliant with the GDPR regulations, especially those operating within the European Union.

Finally, temporary storage of data and data handling are other complex issues posing challenges for RI; data management procedures can be highly variable from infrastructure to infrastructure, depending on infrastructure type. For example, in distributed infrastructure where every facility owns and publishes their own data in different repositories that are subsequently harvested to a joint data portal, or if the infrastructure has a more centralised system where data is stored and published in the one system from the beginning.

Best Practices: Data Management Plan, Standards and Persistent Identifiers

Infrastructures identified some best practices to tackle some of the challenges mentioned in previous paragraph: first, setting up a data management plan; second, implementing persistent identifiers in the metadata catalogues or databases; third, following protocols and guidelines from large and trusted organisations which are most commonly shared within the domain, as that ensures better possibilities of interoperability.

Data Access, Reporting Outcomes and Feedback

Users of Virtual Access access the data by visiting the on-line data repository, searching and filtering the data by different categories and keywords, and downloading the suitable on their personal computer. Some infrastructures may provide helpdesk service or an email contact to advise on the use of the data or if technical problems occur with the download etc.

Challenges: Statistics and Feedback to assess the quality of Virtual Access

Once the data is downloaded, the infrastructure has no information on how the data has been used, if it was employed in any research, if it appears in any publication, and so forth.
Furthermore, statistics on the data usage are very limited since infrastructures must comply with GDPR regulation and therefore can collect limited personal information on the visitors of the data repository. Infrastructures are able to keep records of the number of downloads and the number of visits to web pages, but this information does not help the RI to know about the relevance of Virtual Access as a service, the actual reuse of existing data and its impact on the research environment.

A second challenge identified by the expert group in reporting of the Virtual Access use concerns the collection of user feedback. Some infrastructures do not collect feedback for Virtual Access, while others have set up some sort of feedback collection system into their data repository or portal, but results have been minimal.
User queries are taking place on a voluntary basis, since there is no way to track access, and users are not motivated to fill the query, no matter how short and simple it is. To tackle the lack of feedback, one infrastructure has invented a lottery mechanism to spur users to give a comment on their experience, and similar incentives could be used to gain more feedback from Virtual Access users.

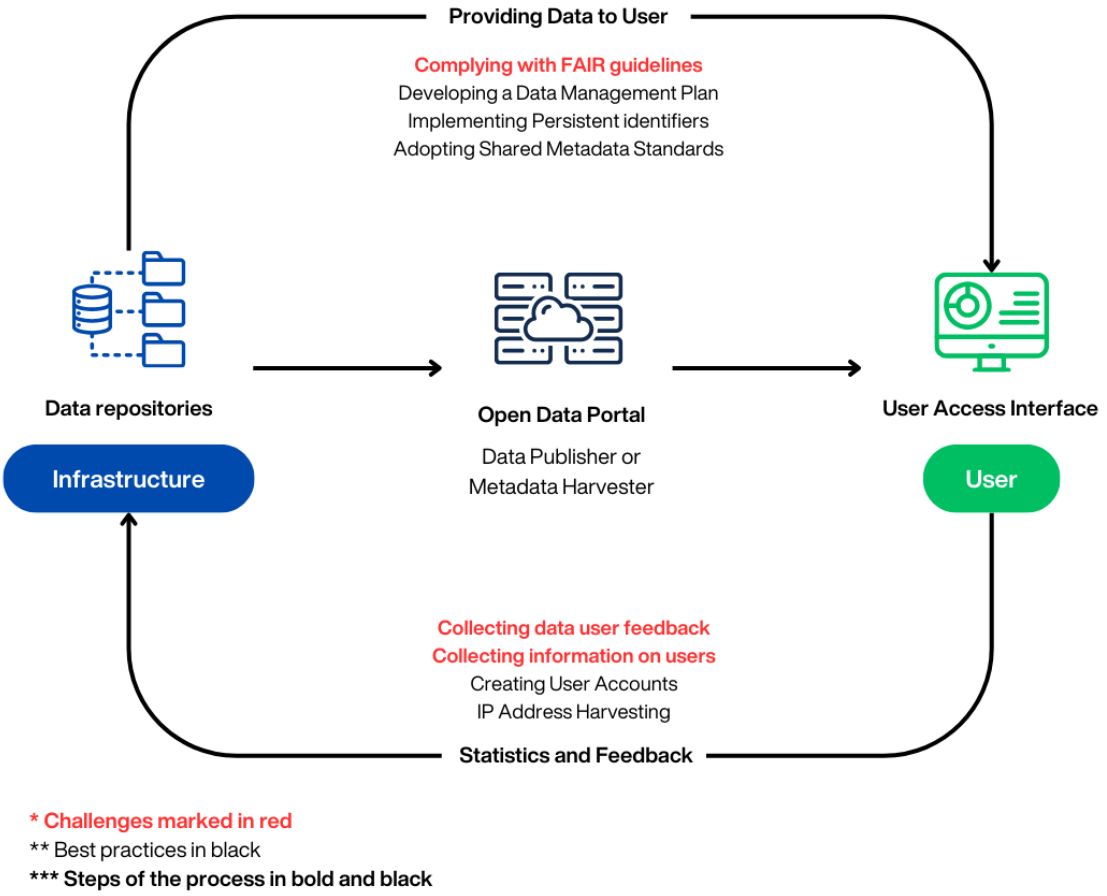
Solutions: Data Licence, IP Address and User Statistics

To improve the collection of publication records deriving from Virtual Access and analysis of user statistics, a good practice is to encourage users to acknowledge the infrastructure for the contribution to their work by giving information on the data licence and provide guidelines

on how to acknowledge the RI in the Virtual Access data repository or portal. Another suggested solution to collect information on the data usage is to implement IP address harvesting.

A possible solution regarding the collection of feedback from the Virtual Access users was asking the users to register to the data repository to download the data (an email address would be sufficient). Users should give their consent to be contacted upon the registration, so that the RI can after a period of time email to the user and to ask their feedback on the service. Such feedback would be extremely more valuable than the feedback received on the data portal immediately after downloading the datasets, as the user had the time to work and use the data, and thus could give more helpful insights on what works best and what does not concerning Virtual Access.

Summary of Quality Assurance Challenges and Solutions in Virtual Access



Conclusions

The Expert Group discussed the Quality Assurance in Remote and Virtual Access provision, with the purpose of identifying challenges and best solutions in ensuring the quality of remote research. Experts in the group enlisted several tools and mechanisms such as quality certifications and external auditors, to support and guide the RI to set up a Quality Assurance program with necessary control steps and to follow shared guidelines to maintain and improve quality of their remote and digital access services.

In conclusion, although Remote Access was performed even before the pandemic, the COVID-19 crisis forced RIs to quickly react by developing and increasing Remote Access and digital access services, when there was no physical access to the RIs. Infrastructures quickly implemented and developed new methods and tools to offer Remote Access, but very understandably their Quality Assurance practices on Remote Access provision were lacking behind, due to the urgency of the situation, or were developed based on physical access meaning the practices were not optimised for Remote Access provision. Currently, the most urgent issues that affect the quality management of Remote Access are cyber attacks and sample shipping, which are both “threats” to the quality coming from outside the RIs. RIs have identified several best practices, like MFA authentication, segmentation of workflows, or bilateral agreement with courier companies for sample shipping, but further developments are needed, such as safer ad hoc designed softwares for remote desktop access and an European framework for RI sample shipments. Experiment protocols and safety evaluation are also weaknesses in the chain of Quality Assurance methods noted by Ris.

Virtual Access provision, on the other hand, presents different challenges, above all the compliance with FAIR guidelines and the lack of user feedback or output. RIs have implemented some solutions, like persistent identifiers and metadata standards, and have discussed new possible ways, like IP harvesting and cyber user accounts, but there is still plenty of room for further collaboration and knowledge exchange in this field to address the current challenges and provide solutions for the future.

Acknowledgements

The Expert Group members are warmly acknowledged for their valuable contribution to the discussions and for collecting and identifying the challenges, best practices and solutions related to Remote and Virtual Access provision.

Annex 1. Composition of the eRImote Expert Group I on Quality Assurance and User Experience.

Name	Institution/Infrastructure	Domain
Ada Pastor	University of Girona	Earth Science
Auriane Denis Meyere	Institute of Structural Biology Grenoble	Life Science
Cecilia Blasetti	ELETTRA Sincrotrone Trieste	Physics and Engineering
Claudia Pfander	Euro-Bioimaging	Earth and Life Science
Deborah Wiltshire	GESIS	Social Science
Denis Gorbunov	Helmholtz-Zentrum Dresden-Rossendorf	Energy, Health and Matter
Ferenc Borondics	SOLEIL Synchrotron	Physics and Engineering
Göran Karlsson	University of Gothenburg	Earth and Life Science
Holger Villwock	SITES	Earth and Life Science
Janez Planec	University of Ljubljana	Earth and Life Science
Jean-Francois Perrin	European Synchrotron Radiation Facility	Physics and Engineering
Joanne Mccarthy	European Synchrotron Radiation Facility	IT
Klaus Kiefer	Helmholtz-Zentrum Berlin	Energy and Matter
Leena Lappanen	Finnish Meteorological Institute	Atmospheric Science
Luigi Paolo D'Acqui	National Research Council Italy	Earth Science
Luisa Cortes	Center for Neuroscience and Cell Biology	Human and Biomedical Science

Martin Chamberlain	European Commission	Research Innovation
Michael Raess	INFRAFRONTIER	Biomedical Science
Mickael Lamay	Centre d'études nordiques (CEN)	Earth, Atmospheric and Life Science
Oriol Grau	University of Antwerp	Earth Science
Pasi Kolari	University of Helsinki	IT