GETTING CONNECTED

How SAIs with limited internet access can get the most out of existing technologies

INTRODUCTION

Many SAIs have limited access to internet, especially when staff are working at home or in remote locations during field work.

Nevertheless, SAIs are finding **many ways of working around such constraints.** This infographic aims to share some of those practices. It is not a "how to manual", for that SAIs will need to turn to ICT experts. However, the idea is that this infographic should **help SAIs think more widely about their options for improving connectivity**.

Also, **think strategically**. The tips in this infographic may be helpful but do not lose sight of the big picture. Make sure that decisions **fit within your overall long-term strategic plan** for the SAI and how information and communications technology will **support your core business.** Make sure all decisions and purchases complement these overall plans.

Where are we now?

What can we do, and how?

What are others doing?

Where are we now?

How is poor connectivity affecting us? i.e. What is the problem?

Poor connectivity makes all external communications difficult, reduces efficiency, and can adversely affect staff morale. If a SAI has limited or poor internet, there are a wide range of activities which it cannot easily do.

These may include:

– Sharing information among auditors when conducting a particular audit.

– Taking advantage of the efficiency of the **cloud-based** systems.

– Accessing the ICT systems of auditees, especially financial information needed for the audit process.

– Operating **efficiently** in the field and capturing auditee data which is only available in hard copy when power supplies are erratic.

– Making it **difficult** to produce audit reports faster.

– Communicating easily with staff who are working at home or away from the capital city.

– Enabling managers to **review** the quality of audits while staff are in the field.

– Participating in global or regional webinars.

– Benefiting from international **e-learning** events.

What do we currently have? i.e. Where are we now?

As part of seeking solutions, SAIs need to do a stocktake, identifying clearly where they currently are.

Some of the high-level areas which should be covered includes:

- Does the SAI have a clear, costed ICT strategy and plan?
- Does the SAI have in place the necessary policies and controls?
- Has the SAI identified the equipment and software it needs?
- Has the SAIs identified the ICT skills it needs

Does the SAI have a clear, costed ICT strategy and plan?

– Where does **ICT** fit in the overall **SAI** strategy ?

– Is there a separate ICT Strategy or **Annual Plan**?

– Has the ICT been costed? Is it in the SAI's **budget** submission to Parliament or the Ministry of Finance?

– Does the budget include the cost of **training**, and the on-going costs of **maintenance** – including recognising that computers need to be replaced at regular intervals?

– Have you identified the **key risks** you might face – dependence on key individuals, theft of equipment, and more damagingly theft or loss of data – and have you considered how to manage such risks?

Does the SAI have in place the necessary policies and controls?

– What external policies and legislation on ICT does the SAI need to **comply** with?

– What policies does the SAI have on keeping ICT information and resources **secure**?

– Does the SAI have policies on the **personal use** of SAI equipment?

– What policies does the SAI have relating to **remote working** and staff using their own equipment?

– Does the SAI have a `**buy your own devices'** policy for helping staff purchase their own equipment, including home internet, security, and back-up generators?

– Does the SAI have systems in place to verify compliance with policies, especially regarding **information security**?

– Does the SAI conduct an annual overall IT audit on the **control environment** focused on key risk areas?

– Does the SAIs have clear policies and procedures in place when **disposing** of redundant equipment, e.g. cleaning out data from memories, and even destroying hard drives.

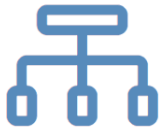
Has the SAI identified the equipment and software it needs?

What is the current state of the SAI's internet? For example, to be able to hold a video conference download speeds of at least 10 Mbps are needed.

What is the current state of the internet in the country i.e., are there organisations and/or places where connectivity is better and if so, can the SAI's access those? (See SAI Remote Working image (open in new tab) when internet connectivity is poor).

How many laptops does the SAI have, what does this work out at per staff member, what proportion of these computers are fit for purpose (i.e. can they do the job the SAI needs them to do), and how long can batteries last?

What licensed software does the SAI use? How many of the laptops have access to this software?



Are the laptops networked? If not, how is information shared between computers? E.g., flash drives, or sent via the internet as email attachments? (See Local area network image)

Do staff all use an email with a common address?

What data storage capacity does the SAI have? Is this sufficient based on the SAI's assessed needs? Can it use the cloud safely; what legislation and/or government guidance exists on the use of the cloud?

How reliable is the electricity supply and, if it is unreliable, does the SAI have back-up generators, solar panels, battery operated equipment, rechargeable power packs?

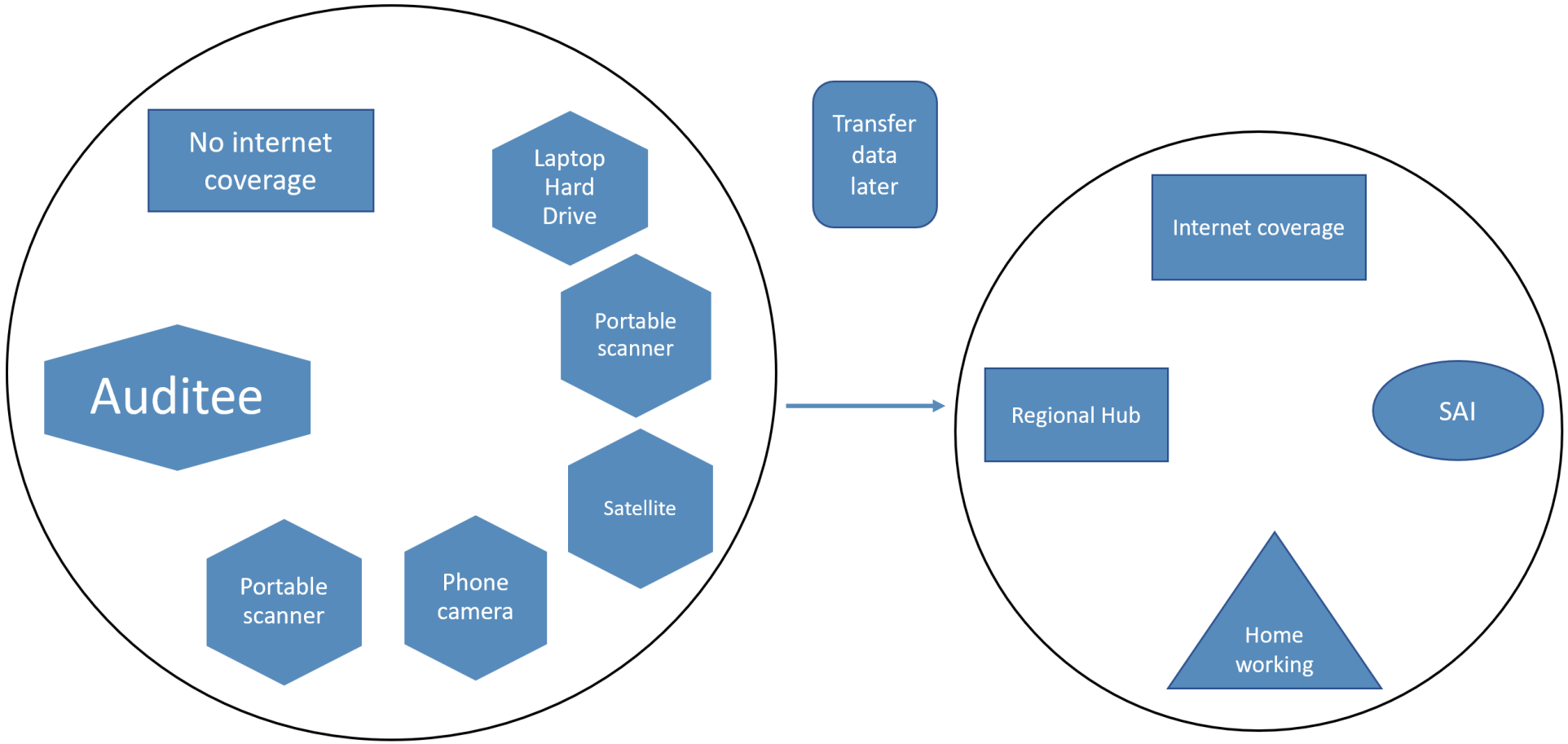
How many mobile phones does the SAI have per staff member? Do they have sufficient airtime to communicate with colleagues and auditees and data to be able to be used to photograph and transmit documents from the field? Can tethering be used?

Does the SAI have any portable scanners, if so, how many? Does the SAI use tablet computers, if so, how many?

Do SAI staff have access to a help line when they encounter ICT related problems? How is this funded?

When computers, phones and other equipment are obtained, details need to be entered onto an asset register which records clearly who has custody of the particular item. Is someone in administration required to check annually the location of all main items?

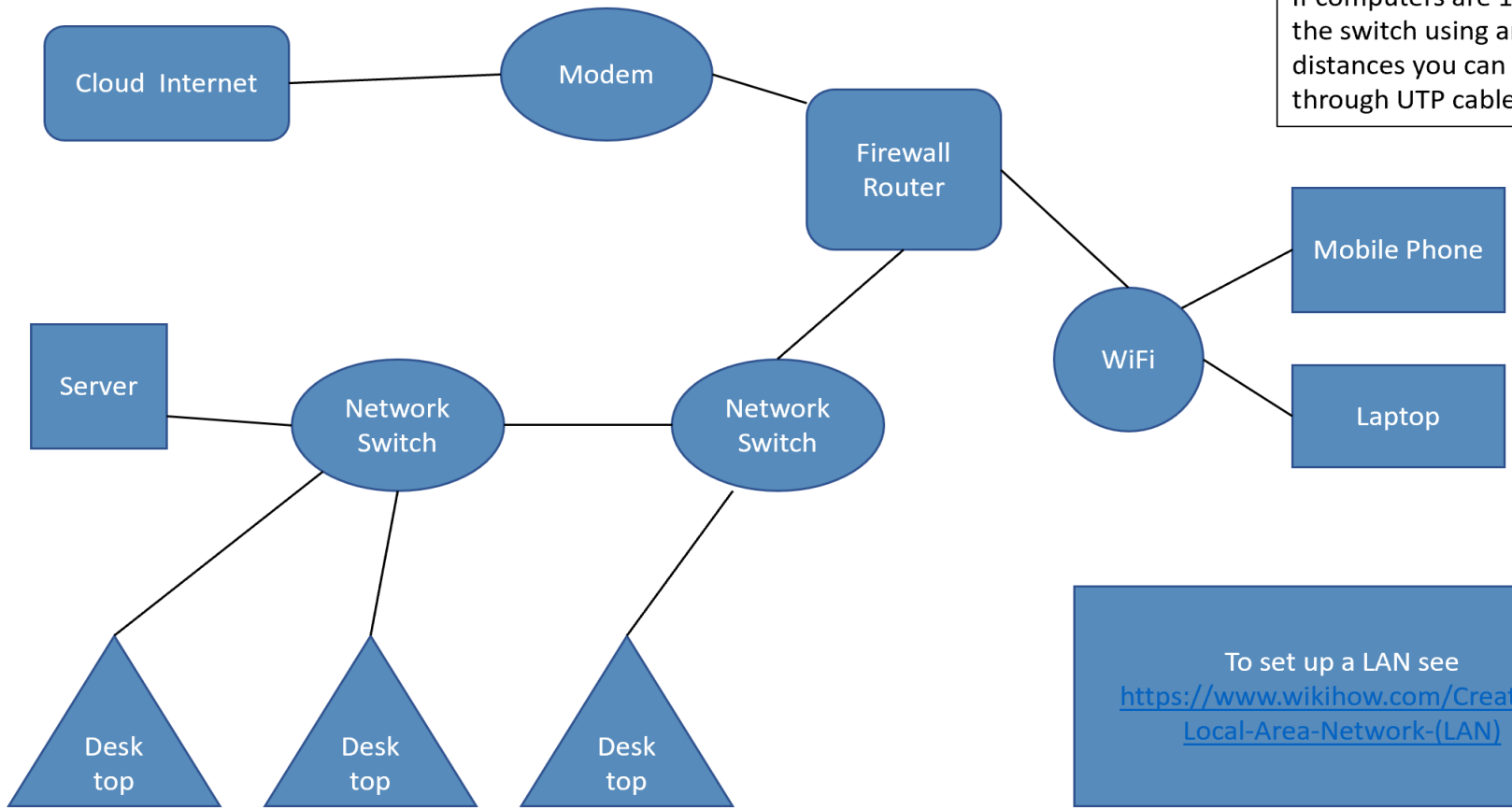
SAI Remote working



SAI Local Area Network

Even if the internet is weak, if the computers are part of local area networks, files can be exchanged using switches.

If computers are 100 m apart they can be linked to the switch using an ethernet cable. Over longer distances you can link switches using straight through UTP cables (or crossover cables).



To set up a LAN see https://www.wikihow.com/Create-a-Local-Area-Network-(LAN)

Has the SAI identified the ICT skills it needs?

Associated with the introduction of new approaches, the SAIs should also ensure that staff are kept informed and understand how proposed changes will affect them

What ICT internet and systems skills does the SAI have?

How many ICT staff does it employ, are these staff permanently available to the SAI, what skills exist in country, in government or in the private sector?

What percentage of staff can comfortably operate core word, spread sheet, and other software packages?

Can the SAI access the advice and support needed?

What specialist ICT skills exist in the SAI?

What can we do, and how?

EXPLORE THE QUESTIONS WHICH INTEREST YOU, TO KNOW HOW OTHERS ARE ADDRESSING THESE ISSUES

- What can we do as a SAI to create an enabling environment?
- How can we ensure the authenticity of electronic evidence?
- How can we make better use of existing internet coverage during webinars?
- How can we maintain contact with staff who are working at home?
- How can we ensure our equipment is safe when working from home, or in the field?
- How can we collect audit evidence in the field when clients' records are paper based?

What can we do as a SAI to create an enabling environment?

Obtain the necessary specialist ICT staff to help create the enabling environment

– Could be via contracts with the local private sector, a short-term external donor funded consultant, or direct recruitment of own staff

– Conduct a benchmarking exercise with peer SAIs – the numbers needed will depend on the complexity of the systems to be managed

Develop a costed ICT strategic plan which addresses:

- Deciding on solutions for data storage
- Deciding on computers
- Deciding on software
- Deciding on smartphones and operator
- Deciding on auditing management software
- Making video conferencing work

What can we do as a SAI to create an enabling environment?

Good contracting practices – make sure there are sunset clauses to check prices are still competitive.

Do not forget…

.. to identify and budget for the training needed by staff, including how to use the newly acquired equipment and software as well as their responsibilities for security of equipment and data

Does the SAI have a common system of defining folder structures so that everyone knows how to label documents and where to save them?

Training for staff, embed within induction training for new staff, and keep training, especially on security.

The SAI's annual training plan should include opportunities for staff to learn how to operate new equipment, and progressively enhance their skills using core software.

Check out the INTOSAI Capacity Building Committee Guide – Managing Information Communications Technology

The on-going costs which need to be built into the SAI budget –insurance, line rentals, replacement equipment, servicing, data.

Remember

ICT is not always the answer. While computerising audit processes can encourage systematic approaches to audit, SAIs need to have in place consistent audit approaches, as well as standardised toolkits and forms which auditors are expected to use. ICT should enhance effective processes, not automate failed approaches.

Deciding on solutions for data storage

Choosing storage options

Own your own

Advantages:

- You control the security
- No need to worry about internet connection (in the same office)

Disadvantages:

- Highly technical and not all SAIs can afford to employ the necessary ICT skills
- Costly to install and maintain
- Bulky
- Needs to be in a secure, temperature controlled, area in the SAI
- Risk of loss of data in an emergency – flooding, earthquake, civil unrest
- Still needs back up off site every day
- Limited access right

Storage in the cloud

Only possible if government rules permit. There may be national/local cloud-based storage providers that fulfil the government's rules, where global providers do not.

Advantages:

- Resilience – data unlikely to be lost
- Additional data storage, generally easy albeit at a cost
- Backed up automatically
- Software updates

Disadvantages

- You are dependent on the security of the provider and the country where the storage physically occurs
- Overall costs may be higher and additional data storage expensive
- If you do opt for the cloud, there are ways of improving security:
  - *Systems such as Microsoft One Drive for Business can be made safe with a combination of using strong passwords, two-factor authentication, and made safer still by using such software as Box Cryptor.*

Dongles – usb routers – to access internet when working remotely – not so widely used now but can be helpful. **Costs** can be managed by agreeing with the provider usage limits. **Training** should be given to staff on how to manage data consumption.

Flash drives –come with **risks** because they are easily lost. A larger portable flash or hard drives may be more helpful and can store more data.

Tablet devices – look for up to 10 hours of battery life (manufacturers often exaggerate), at least 2GB Ram, operating systems choice between Google **Android**, and **Apple**, get biggest storage size you can, quad core processor higher GBs better screen size 7-8 inch smaller are more portable but if you plan to use them as a work tool then a larger 11 inch one may be more practical.

Deciding on computers

Consider buying a mixture of computers – some staff may not be handling large files with massive amounts of data – so consider obtaining good work horse computers and just a few top-of-the range ones.

Points to consider when buying computers

Specifications for every-day computers:
-At least – Intel Pentium, Core i3, AMD Ryzen 3, at least 4GB Ram, and a Solid-State Drive (SSD).

Specifications for heavy data users:
– Intel Core i5, i7, AMD Ryzen 5 or 7, 8GB of Ram or more, and a SSD.
– Operating systems – mostly a choice between Windows and MacOS.
(***Windows 10*** – *greater range of specialist software, more choice of laptops.* ***MacBook*** – *for longevity and quality but more expensive.* ***Linux*** *based operating systems (in practice Ubuntu) are low-cost and place lower demands on the computer though less widely used than the other.)*

Screen size and weight:
Bigger is not always better – go for 11, 12, or 13 inch display which typically weighs between 1 kg and 1.5kg. However, if weight is not an issue the larger 14 or 15 inch screen computers are often cheaper. Go for a Full-HD 1,920×1,080-pixel resolution display – it will be sharper and cause less eyestrain.

For everyday use and to save the backs of staff – consider using separate monitors with larger screens which can then be set at people's eye levels. Be careful about ultra-light computers they may not be robust enough for traveling around the country.

Other considerations:

- Camera – usually now built in.
- USB ports – useful for back up, presentations, but some SAIs block for security reasons and to avoid unauthorised transfers of data.
- Long battery life – for those which will be taken to remote locations – 24-hour battery life is ideal. Manufacturers often exaggerate the life of their batteries – check with local reviews.
- Robust case – ideally lockable and able to be locked to something secure.
- Warranty After-sales support.
- Would you want some apps pre-loaded?

Deciding on software

Issues to consider

FUNCTIONALITY
word processing, spread sheets, email, presentations, data analysis, meetings

INTEROPERABILITY
ability to interact and share data

DELIVERY MODEL
local or cloud, for example – again balance of resilience vs bandwidth available

AVAILABILITY
of online help desks and support services

COST
per month and per device

Obtain a multi-user contract with a software provider – e.g. **Microsoft** Office Business Premium or Standard, or **Google** Workspace. A free alternative is **Libre Office** which comes with its own word, spreadsheets and slide programmes. This can be augmented with a free email system such as Mozilla's Thunderbird.

Anti-virus protection – often comes with office software but an antivirus software which mitigates internet threats is recommended. In many cases the bundled security manager Defender in Windows is good enough. However, it is always important to **train staff** in "security awareness". When using Linux there is no need for antivirus software, at least for the moment.

Selecting an operator:

Select an operator which can provide:

- Best 4 G coverage across the country
- Speed – a minimum acceptable upload and download
- Reliability – how often does it drop out?
- Best price for data and for duration of calls
- Specify what is needed from them in terms of SAI network
- Guaranteed levels of service and refund arrangements should the level of service not be provided
- Ease of payment by the SAI, and cost of additional data and users
- Consider installing fibre optic cable in HQ
- Ensure that the internet bandwidth is 15/15 Mbps
- Security
- Ease of contracting

Consider negotiating with the network provider to create a closed network – are the network calls likely to be free calls i.e., staff to staff with a small charge for external calls to clients and others.

Choosing phones:

- Cost – famous brands come with a premium.
- Good battery performance (speed of charging, battery lifetime, spare batteries, and ability to change may be worth considering.
- With android phones, you need at least 3 GB of primary and 32 GB of secondary storage.
- Ease of finding and cost of replacing chargers and leads (notoriously liable to be lost or misplaced).
- Good storage capacity.
- Compactness (fit in a pocket), not always need big screen or latest cameras.
- Robustness.
- Warrant.
- Good cover/screen protector – flip covers

Deciding on smartphones and operator

Deciding on audit management software

AT FIRST

– Ideally put in place good paper-based audit management system. However implementing an AMS can encourage greate audit consistency.

– Select computerised auditing software which is **consistent** with this approach.

– Keep solutions **simple** and in line with the ICT maturity level of the SAI.

– Consult with peer SAIs that have such software and could help with **training**.

-When developing solutions, consider change management and keep **stakeholders** on board.

KEEP IN MIND

Does the audit software operate on a phone or different operating systems or browsers? If staff record documents on their phones, who owns the data, where is it stored, and if the staff member leaves can we be sure the data is wiped? May not be a problem with open domain information, or auditee materials which can be obtained by the public easily but for more privileged material creates a risk.

Consult with peer SAIs that have such software and could help with training.

Deciding on audit management software

Off the shelf

Advantages:

– Usually tried and tested system – more advanced functionality, more system security incorporated

– Available experiences from SAIs (or organisations) which have used the audit management package

– Usually, such software has better support and online user forums to share experience and respond to FAQs

Disadvantages:

– Difficult or impossible to incorporate SAI specific needs

– Usually tailored more to operating environments of private sector audit

– Usually more expensive in implementation and annual licence fees

In-house developed

Advantage:

– Can add specific SAI needs in the development of audit management systems

Disadvantages

– SAI may need internal staff to maintain software or continue engaging a consultant

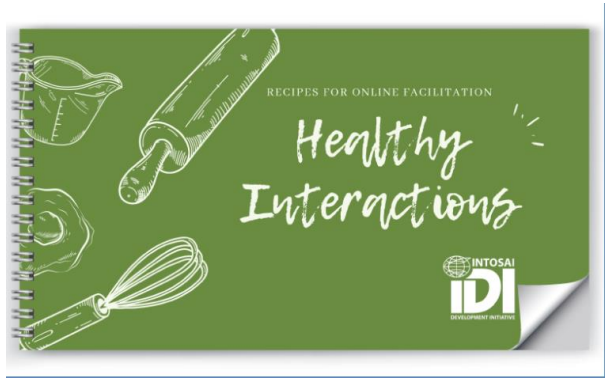
– Can be time-consuming and costly

– System resilience and security may not be fully developed (or take time to get right)

Making video conferencing work

In recent years, many SAIs have begun to use video conferencing packages such as Teams, Zoom, Google Meet and Blackboard to connect both within a country and especially internationally. Poor internet connections can make this difficult and frustrating, and good lines are rare with less than 2 Mbps download speed.

However, there are many simple techniques which can help to make things better including:



CLOSE OTHER APPLICATIONS

Setting up a large screen and microphones in a training room and inviting interested colleagues to gather round one connection point and turning off internet connections elsewhere in the office

USING SOUND ONLY

Using mobile phone connections

– though this can be expensive

Moving close to the router or other places in the SAI where internet coverage may be better

Listening to the webinar on the premises of other organisations with better internet connections including hotels, international donors, and multi-national companies.

How can we ensure the authenticity of electronic devices?

Increasingly SAIs want to access documents provided by auditees **electronically**. In doing this SAIs need to be able to guard against tampering and be assured by the auditee that the document is authentic.

Some SAI may need to amend their **legislation** to accept electronically copied documents.

Procedures need to be agreed with audit clients, staff need to be trained, and internal auditors need to occasionally confirm that the controls are operating as intended.

A digital mailbox can be used to for sending, signing, and **certifying** information using an Advanced Electronic Signature which comes with a time stamp to assure integrity.

Alternatively, though **less secure**, auditees can be asked to sign and date stamp copies of key documents and scan them into such software packages as Adobe, or Docusign, or save them into PDFs

(SAI Nepal can photocopy documents on the auditees premises but for key documents will ask the auditee to have the copies signed and date stamped to avoid the risk of future disputes. Documents sent in this way need to have end to end encryption using such apps as: Signal, Spider Oak, pCloud, Resilio or Engimai)

Switch on audit logs (i.e. records of access and amendments to documents) so there is a **record** of amendments and access. Audit logs should be reviewed regularly and at the appropriate level. This should be done for Audit Management Software and system administration.

Some handy tips which may help:

- Use headphones to cut out extrinsic **noise**
- Turn off other programmes to reduce interference
- Turn off other internet connections nearby to **reduce the local traffic** on the net
- Listen to the webinar on one computer, perhaps in a training room, to reduce the number of access points
- Install generators or solar panels to ensure **reliable electric** supplies
- Schedule webinars at times when there is lower internet usage in the SAI/country (when typically, is that?)
- Move to the offices of donors or to international hotels where the internet is stronger
- Connect your computer **directly to the router** using an ethernet cable assuming the router is connected to a broadband cable or fibre optic
- Invest in boosters to enhance the connectivity in rooms some distance from routers
- Always **mute** when not speaking
- Turn off video links and just rely on sound, especially if you are not presenting
- On sharing webinars, you could cast or share your screen onto a larger modern TV. There are also 'plugin' devices for older TVs that allow you to cast a laptop screen to them.
- If the internet coverage is too poor, consider **phoning** in using Whatsapp or a similar app

How can we make better use of existing internet coverage during webinars

How can we maintain contact with staff who are working at home?

To work around poor internet cover at home:

Do not expect immediate responses, allow for asynchronous connections

Send key documents overnight when internet usage is low

Use mobile phone tethering at off peak times to send and receive documents and use metered connection when tethering or have limited Wi-Fi

If the SAI has negotiated a closed phone group contract with the service provider, then it is likely that calls in the network i.e., staff to staff, will be free and external calls to clients etc will only incur a small charge

See SAI Uganda case study.

Staff provide own equipment to specifications provided by SAI and then staff receive a contribution towards such costs.

Need to be a clear SAI policy.

SAI will need a to agree level of contribution and arrangements should the phone be lost, or the staff member leave the SAIs

Arrange for the phones to be topped up monthly with an agreed volume of data usage

Ensure staff know how to keep data usage to a minimum

Create common emails:

If there is no current system of common emails, create a network with common email addresses (Gmail, Microsoft, Yahoo, or another common email provider)

You may consider setting up a separate email-domain (saicountry.com) on a web-hotel/hosting provider. May be more cost-effective and give more options

To help staff who have erratic electricity supplies

Contribute to the cost of home generators via perhaps a loan scheme and/or provide extra batteries which can be charged off-peak

Issue staff with smart phone

Consider the following: Preload a prepaid monthly allowance for data use and phone time. Resolve issue of who pays for personal phone usage

Issue staff with laptops

Allow staff to use for a small number of personal calls:

Check if there are any tax implications

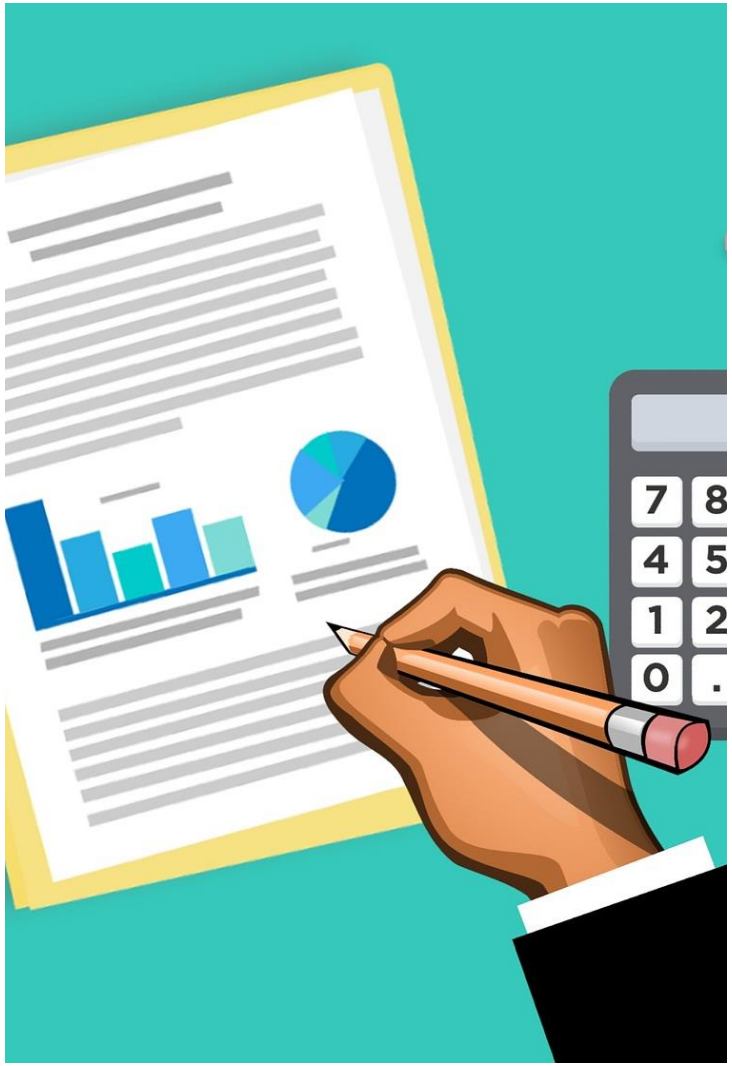
Adopt an honesty policy with staff paying the SAI monthly for personal use (with occasional spot checks by SAI Internal Audit)

How do we ensure our equipment is safe when working from home, or in the field?

Ensure all devices are encrypted – most devices can be bought pre encrypted. Remote storage devices sometimes come encrypted by default. If they do not, commercial file encryption packages can help. Windows also has the ability to encrypt files. There are a range of options here for sensitive materials. You need to be clear on the encryption key (password) though – you are really trying to save the data from a casual thief (so consider a key per audit or similar).

Windows devices are often encrypted by default (you configure the device with Bitlocker on setup Device encryption in Windows 10 (microsoft.com). This is not the case for Windows 10 home.

– Always enable **security locks** in laptops and phones, i.e. use a password or fingerprint or face-recognition graphics.
– Follow security protocols provided by HQ.
– Keep devices **out of sight** when travelling on public transport.
– **Lock** the devices away at home when not being used.
– When working on a client's premises, lock the computer to a secure place and never leave it unlocked on a desk, even if going to the bathroom or for lunch. (*Keep devices locked away in a safe in a hotel, or chained to furniture*).
– For sending messages use free cross-platform encrypted **messaging service** apps e.g Signal.
– Devices can be wiped remotely when they are registered to an account.
– Purchase devices which are **GPS trackable**, for recovery, and make sure it is switched on. (*Consider whether it might be more efficient for staff to have the capability to do this so they can turn this feature on when they are in the field as well as having it centrally controlled.)*
– Establish clear security and **safety protocols** for keeping equipment safe, keeping data safe, keeping staff safe, and again keep training.



– **Ensure** that your legislation accepts electronic and/or photographic records as evidence – if not seek to have the law amended.

– **Issue** back up batteries and chargers and use battery operated portable scanners.

– **Back up** audit files on a USB stick, floppy disc or portable hard drives and courier to nearest point with strong internet – a regional government hospital, a regional SAI office or even the SAI head office.

– **Locate** internet or satellite points where audits can be uploaded and shared with audit managers in a SAIs headquarters – may be too expensive in most cases for a SAI to own and/or use.

– **Use** smart phones to photograph auditee document:
(Ensure that the phones indicate the time, date, and location where the documents are photographed. Camera settings should have location tag settings switched on.)

– **Download** an Optical Character Reader (OCR) app on to the phone or tablet and use to convert from JPG to PDF to Excel. *(Camscanner allows iOS and Android devices to be used as image scanners. It allows users to 'scan' documents and share the photo as either a JPEG or PDF.)*
(Reduce the file size of photos – switch from colour scan to greyscale one and reduce its quality to the least tolerable level.)
(Possible tools for images include: https://sourceforge.net/projects/flexxiimage-resizer/ or https://www.xnview.com/en/ or GIMP https://www.gimp.org/.)

How do we collect audit evidence in the field when clients' records are paper based?

What are others doing?

CASE STUDIES

SAI Tunisia:
A networked office starting to use IPADs

SAI Uganda:
Incremental improvements

Lessons from the ACCC webinars

SAI Kosovo:
A small SAI with a strong IT backbone

SAI Nepal:
Linking up the bits

SAI Kosovo – A small SAI with a strong ICT backbone

Over the past 10 years, SAI Kosovo has invested heavily in creating a strong IT capability to support its audit staff, and this played a major role in facilitating home working during the lock downs arising from COVID 19. All staff are equipped with laptops which have core i5-i7 processor, 4-8GB RAM, 500GB-1TB storage, and Windows 10 operating system. They are loaded with Microsoft Office 2016/365 provided through a government wide centralized licensing contract.

The laptops are networked through a domain controller administered by the IT Department. SAI Kosovo has its own servers, including: File Server, Active Directory, Mail Server, Storage Server, Database Server, and Application Server. It also has the necessary network resources, including a firewall to ensure a secure connection from the internet to the internal network. The access to the internal network for all staff is provided through the FortiClient application, which uses encryption, and a digital certificate installed in all laptops to secure the connection from the internet to the internal network. Digital certificates are electronic credentials that bind the identity of the certificate owner to a pair of electronic encryption keys, that can be used to encrypt and sign information digitally. In SAI Kosovo's case, they are using FortiClient – SSL VPN with certificate authentication. It is configured with FortiGate as CA (Certificate Authority) connected with its domain controller to authenticate users.

As SAI Kosovo has its own mail server, it has been able to send and receive documents from audited entities, without problems during the pandemic lockdown. Digital signatures are not yet in use in government, so SAI Kosovo has equipped auditors with portable scanners when they are in the field so that when necessary they can capture audit evidence which has not been stored electronically.

However, this is rarely used as most audited entities have their data in an electronic form. Where documents were received through the official e-mail of the Republic of Kosovo, in the absence of digital signatures, the documents are signed and stamped by the responsible persons in the entities, scanned, and then sent to SAI Kosovo.

During the pandemic lockdown, SAI Kosovo developed and implemented a new Audit Information System, SITA, based on its audit methodology. Initially, all audit processes were identified, and this system was developed based on these processes. The key requirements for the development of this system were to digitize and centralize all documents and working papers to automatically align all phases of auditing and generate final documents on the basis of data and tests carried out at different stages of the audit process. This system ensures that the SAI's audit methodology is applied more effectively, productivity is increased, and the quality of audits is assured, particularly when undertaking complex audits which require high levels of assurance and adherence to the standards, laws, and regulations. It provides auditors with faster access to information, a wide range of audit methods and tools, and, compared with traditional working methods, carries out more effective and efficient audit calculations. SITA is a web-based application implemented on the SAI's internal network. Access to the system internally is through the Active Directory with Single-Sign-On, and access externally via the internet is provided when a laptop operating from outside is granted access to the internal network. When implementing SITA, it was necessary to add extra servers and introduce new tools to strengthen backup. A centralized log management server has also been installed at the same time, increasing the system and network security.

Internet coverage is good across Kosovo in all public institutions, most individuals have affordable internet coverage at home, and telecommunications companies offers 4G network at a reasonable monthly cost. With this infrastructure, SAI Kosovo was able to hold team meetings and meeting with audited entities through Zoom.

One of the positive impacts of Covid-19 for the SAI has been to encourage much greater use of IT tools, and to give greater institutional recognition to the critical importance of a well-staffed and well managed IT department. As a result, and despite the lockdown, the SAI has achieved its annual plan and published all reports, within the extended deadline provided by the Assembly of Republic of Kosovo.

For further information please contact: Qendresa Mulaj on qendresa.mulaj@oagks.org

SAI Nepal – Linking up the bits

SAI Nepal has many of the IT components needed to be a fully networked office, but it is still work in progress. Most of its 350 professional staff have laptops but many of these are now old and lack the technical features needed to work on large databases. While the preferred platform is Microsoft Office only the 50 to 60 most recently purchased computers come with Microsoft Office installed. For reasons of cost and age of computers the SAI has not been able to roll this software out across the whole office. However, in part there is still a need to convince staff of the need to use approved and licensed software. Data are stored by staff on their own individual laptops, i.e., on their hard drives. Some staff back up this data on external portable hard drives, and/or flash drives, though others have started to store files in the cloud using Microsoft One Drive. Data are shared from one computer to the next using flash drives, emails and/or USBs. The SAI is not currently networked, and data are not stored in a common location either in the cloud or on the SAI's own servers. However, an external consultant has been funded by the World Bank and plans are being drawn up to introduce a Nepal Audit Management System and create a networked office .

The office has 3 IT staff who are involved in developing and supporting the IT communications. However, these staff are part of a government pool of staff. They are not employees of the SAI and are generally rotated every two years to other departments, setting back any attempts at long term planning and improvements.

Nepal has a functioning national internet network which reaches all 77 district-headquarters. At times, this internet is understrength and slow, but it is adequate for staff when they are out on field audit and they are able to maintain contact with the main SAI office in Kathmandu. There is a government email system with its own domain. However, the SAI finds this too slow, and has set up a common email group for all staff using google gmail.

The SAI does not provide staff with mobile phones but instead expects them to use their own phones when outside the office. The travel and subsistence budget contains a small allowance for miscellaneous expenses, and this is expected to cover the cost of work-related calls. Most of the auditees now have computerised records and SAI staff can access these when on local audit and download the files they need to complete their audits. In the rare cases when the audit files are still paper based, staff can photocopy the needed documents and have the documents signed and date stamped by the auditee as authentic copies. This is done if the SAI auditors believe that there a risk that audit evidence might be altered and/or to avoid future disputes.

SAI Nepal uses zoom and google meet for video conferencing and this has been a major help during the current crisis.

Security of computers is the responsibility of individual staff. However, while the SAI has security policies in place, compliance with the policies is not systematically checked.

For further information please contact: oagnep@ntc.net.np or hrd_ir@oagnep.gov.np

SAI Uganda: Incremental improvements

In all but the most remote parts of Uganda, internet connectivity is fast and effective. In recent years, the Government has installed a national fibre backbone connecting all major centres, making it easier for SAI Uganda to conduct audits across the country. But it has not always been like that.

In the early 2000s. SAI Uganda had only one laptop for every 4-5 staff, mobile phones were only held by senior managers, regional offices were not connected to the internet, and field work was predominantly paper based. As part of the process of implementing its dream of accessing a modern IT enabled audit environment, the SAI recruited a small specialist IT audit team, created a local area network in its head office, progressively acquired more laptops, installed servers, purchased a licence for Microsoft Office, used Microsoft Exchange Server to create its own email domain (@oag.go.ug) for all staff; and used Outlook for external client access.

When buying laptops one prerequisite for those the SAI planned to use in remote locations was that they had to have powerful batteries capable of lasting for 24 hours for effective working in areas off the grid or subject to regular outages. To do this they bought spare battery packs.

To work remotely, the SAI purchased 500 smart phones, one for each member of staff. The mobile phones were chosen on the basis of their durability, the quality of their cameras and affordability.

In selecting a telecom provider, a core requirement was countrywide coverage, and they had to be able to demonstrate that to the SAI. An agreement was struck with the provider, and sim cards provided, to create a closed user group i.e., a group comprising all the 500 new phones with an agreed annual tariff which meant that any calls between the phones on the group were at no extra cost. To avoid staff having to carry multiple phones, a small additional allowance was provided for staff to use the phones for personal purposes. In addition, the SAI purchased a data bundle from the provider so that each month all phones received a 15 Gigabyte of data. This volume has been found sufficient to operate the audit management package used by the SAI, namely Teammate.

The TeamMate version being used had a client server model. However, because the SAI has its own servers, it has agreed with the telecom provider to be given its own Access Point Number (APN) rather than go through the cloud to access files. Using its own private network has provided the SAI with a degree of additional security.

When staff are away from their head office in Kampala or their regional offices, or in situations where there are no internet connections, they can connect their laptops to the main system by tethering their phones. Restrictions, however, have been placed on the laptops to mitigate the risk of un-sanctioned applications being installed. There are still parts of the country where there is no internet connection. For a while, auditors took portable scanners with them on remote field trips, but these needed reliable electricity to operate effectively. Instead, staff now rely of their phones during local audit to take copies of key audit evidence, recording their audit findings on their laptops. Each phone is preloaded with the app, Cam Scanner, which converts documents into PDF form, a form which is easier to send via the internet, unlike photographs which are data heavy. Increasingly, even on auditee premises in remote areas of the county, staff have computers so the SAI auditors can obtain copies of relevant documents saving them onto USB HDDS and/or pen drives. These can then by uploaded and shared with audit supervisors and managers based in Kampala when staff return from field audits to their regional offices, which are all now connected to the national network.

SAI Uganda has appointed an IT security officer who is responsible for regularly reminding staff of the importance of safeguarding their computers and data, not putting the computer in the luggage rack on public transport, for example, or not leaving it on a desk in an auditee's premises when he or she visits the bathroom.

During lockdown, and where internet connectivity is good, the SAI has used zoom and other video conferencing packages to save the costs of travel.

For further information please contact: fabian.tonda@oag.go.ug

SAI Tunisia: A networked office starting to use iPads

SAI Tunisia is a networked office in which all staff have access to laptops which they can use in the field and at home. While staff are not issued with mobile phones, they have recently started to use IPADs.

Choosing laptops:

SAI Tunisia use the following criteria when purchasing laptops:

- Intel Core i5, or the more powerful i7 processors
- 8 gigabyte RAM capacity
- 1 Terabyte hard drive

These laptops are all loaded with licensed versions of Microsoft Office.

The laptops currently meet most of the SAI's requirements, but they are looking to acquire more sophisticated laptops for analysing larger data sets.

The SAI employ a private firm to manage its IT services including the provision of 9 employees (4 analysts, 4 technicians,1 senior technician), and back up servers. In choosing the firm the criteria used included the company's prior network management experience, company references, evidence of appropriate certification, including safety-related certification, and the availability of engineers who had the technical skills and a minimum of 5 years network experience.

SAI Tunisia uses the same national internet provider which provides internet to all parts of the public administration. It covers the whole country, so even if there is no internet access in some administrations, auditors have internet access via their mobile phones (4G)

Keeping in touch with staff when away from the SAI

Staff use Outlook to communicate and exchange documents both within the SAI and when on auditee premises.

In the SAI office, staff have access to fixed line phones, but staff are not provided with mobile phones. Some staff use their own personal ones to make calls when they are away from the office and to photograph documents if necessary.

Recently the SAI has issued tablets to all staff. They were a donation from the World Bank to help the SAIs in auditing the financing of the legislative, presidential administration and municipal elections. It can be used to read document, act as a phone (by adding a SIM card), or communicating via WhatsApp, Skype, and Messenger.

Access to working papers

When staff are on auditee premises, they can access working papers directly, photocopying or photographing them, as necessary. Usually, they send large documents electronically using Google Drive. If not, the SAI downloads its documents on to CDs.

During lock down when staff were working at home, they either take the paper documents with them from the SAI Office or ask the auditees to post them. The SAI does not use scanners.

Video conferencing

SAI Tunisia uses Blackboard for plenary assembly meetings, meetings of the President, the meetings of individual chamber, regular meetings with audit staff as well as ARABOSAI meetings.

Security

SAI Tunisia uses the Kaspersky antivirus programme and are given back up support by the IT staff as needed. Security of equipment away from the office is the responsibility of staff but it is a challenge when equipment is used in people's homes, the premises of auditees or is being carried in public places. There are data risks also when working on public networks.

The SAIs relies on auditors' vigilance and support from IT staff who regularly check and confirm the security of documents and computers and advice auditors as necessary.

For further information please contact: info@courdescomptes.nat.tn

Lessons from the ACCC webinars

Presentation tips:

Be Creative

Unlike in an in-person presentation, slides are the main focus therefore fill them with colour, graphics and relevant pictures.

Keep Slides Moving

Add more slides than you usually would and keep the slides moving at a quicker pace.

Make the Presentation Interactive

Have focused discussion topics interspersed throughout presentation to keep listeners engaged.

Use creative approaches to engage listeners through using raised hand icon for yes or no questions.

However, bear in mind that it is difficult to have a full discussion in a webinar, therefore keep discussions specific and focused.

Engage with practical experience of participants

Illustrate points with relevant and practical examples

Keep an eye on the time

This is especially important if there is more than one presenter.

Focus on presenting

IDI will provide support for technical issues, and the facilitators will manage the session and monitor for questions. Therefore, the presenter can focus solely on presenting.

Before the webinar – Checklist

Team Roles

Presenter(s): Deliver presentation and answer questions

Facilitators: To organize the webinar and assist the presenter(s)

IDI: Technical support

Platform: Blackboard

Send out Invite

- Lead facilitator:
  - Agree webinar theme, recruit presenters, and agree date – checking it does not clash with other important INTOSAO events and the availability of the other facilitator and the technical support.
  - Inform colleagues of the time, date, topic, name of presenter(s) and link to Blackboard.
  - Also ask for questions they would like answered on the topic as well providing them with a short description of what the webinar will contain and some background reading.
  - Important to check the time chosen is optimal for the largest number of participants across the world – typically around 1 or 2 pm European time.
  - Arrange a trial presentation.
  - Plan for how you would manage the webinar if there is a power failure or the lead presenter suddenly become unavailable.
- Support facilitator:
  - Advertise the webinar on the IDI website.

Prepare Presentation

- Presenter(s):
  - Give yourself time to prepare and practice your presentation. If more than one presenter, ensure you keep each other up to date on progress.
  - Send presentation to lead facilitator a week before the webinar.
  - Make sure that you have a reliable internet connection – if you are uncertain consider using a location in the country with better connectivity.
  - Use headphones when presenting.

Test Run

- Technical support:
- Send out the Blackboard link to the presenter, providing the capacity to move the slides
- All:
  - Set up a test on Blackboard with IDI technical support prior to the webinar. This will help you familiarize yourself with the software. In this test also check your internet connection, your audio is loud, clear and without echo; your slides work smoothly and check interactive components. Finally practice switching between presenters and muting and unmuting participants.

Send out Reminder

- Lead Facilitator:
  - A few days before and on the day, in the morning, send out a reminder of the webinar.
  - Inform participants that when they log on, they will be muted and not have video access, but they can ask questions by hitting the button to raise their hands or by sending a query via the chat box.

Right before Webinar

Presenter(s), Lead Facilitator, Support facilitator, Technical support:

Prep your Computer

- Close bandwidth-hogging applications, backups, and other resource-intensive processes on your computer. If you're running Dropbox, pause the syncing during your webinar.

Avoid Distractions

- Turn off all notifications from email, social networking tools, backups, etc. Anything that dings, flashes, flashes, or beeps on your screen. Also remember to put your phone on silent.

Arrive Early for Webinar

- Sign onto the webinar around 10-15 minutes early to give yourself time to settle in.

During the webinar

Presenter(s):

- Deliver presentation, move slides, and answer questions.

Lead Facilitator:

- Welcome participants, introduce presenter(s), remind people that the webinar will be recorded, and put on screen the caveat regarding sharing of information.
- Remind participants that the workshop recording, summary, and slides will be sent to them all after the webinar and placed on the CBC website.
- Start recording.
- Facilitate Q/A sessions.
- Wind up session and thank participants.
- Turn off recording.

Support facilitator:

- Monitor chat box for questions and technical issues, send the key questions to the presenter and lead facilitator by email, and prompt to make sure these questions are addressed.

Technical support:

- Mute and unmute as needed.
- Block the pop-up notifications when participants enter and leave.
- Advice on other technical issues as needed.

Post Webinar

Support facilitator:

- Check all questions in chat box were addressed, if not then send them to the presenter and ask for a short note in response to those questions which can be shared with participants – if easier do this by phone/social media.

Presenter(s):

- Answer any unanswered questions

Technical support:

- Send recording of webinar to lead facilitator

Lead Facilitator:

- Produce a summary of the session and clear with presenter,
- Send the summary with other materials and recording to the Support Facilitator to lodge on CBC website
- Send email thanking participants along with summary, recording and slides, invite them to send any evaluative comments, suggest future webinars and or other possible invitees.

Sources of advice and resources INTOSAI

INTOSAI Capacity Building Committee | Managing information communications (intosaicbc.org)

Healthy Interactions - Recipes for Online Facilitation Flipbook (idi.no)

AFROSAI-E Working Group on Information System Audit and Management (WGISAM)

ITSA & ITASA - EUROSAI IT Working Group (eurosai-it.org)

Other sources

ISACA (the IT auditors institute) Local Chapters. There are chapters in most capitals of the world, large regional centres and private sector firms in country.

For specialist technical support and advice see ISACA COBIT

Embassies – for guidance on funding support

International development partners – World Bank and others – for funding assistance

Other SAIs – for technical advice and support