



# THE FOOTAGE WHISPERER

"SEE WHAT THE CAMERA SAW"



**AUDITORS' FORENSIC  
TOOLKIT:  
COM-SUR™ SIMPLIFIES  
SURVEILLANCE VIDEO  
INVESTIGATION**

**WELCOME**



**OPENING THE FOURTH EYE**

Webster's dictionary defines 'audit' as 'a methodical examination and review'.

An auditor is a person, or a firm appointed by an organisation to carry out an 'audit'.

The primary function of an auditor is to ensure compliance with rules, regulations, procedures, operating practices and other such criteria of an organisation and/or as laid

down by law. The auditor, on completing the audit activity, documents his/her audit findings in a report.

Think of Auditing as the Fourth Eye. It's time to open it!

**IMPORTANCE OF VIDEO IN AUDITING**

While the concept of using live or recorded video to carry out remote auditing/inspection was well-known, it has gained paramount importance in the wake of the COVID-19 pandemic. Several top auditing bodies across the world are now adopting remote video auditing/inspection/investigation.

Generally, the following technologies are used in a remote video auditing /inspection /investigation activity:

1. Video calling/conferencing software like

Skype, Zoom, Microsoft Teams, Webex etc.  
2. CCTV cameras  
3. Body worn cameras  
4. Helmet cameras (in industries like mining)  
5. Drones/UAVs  
4. Handheld devices (tablets, smartphones etc.) for capturing still images and sharing with the respective auditors/inspectors.

Also, it is known that some organizations make use of specialised CCTV systems to carry out 'remote video inspection' of structures, equipment, and components that are otherwise inaccessible to a human inspector to physically carry out such activity due to reasons such as their physical configuration, safety concerns, or other limitations. Additionally, organizations also make use of a technique known as video exposure monitoring (VEM) in order to evaluate the various 'exposures' to potentially hazardous substances like chemicals, dust, exhaust, radioactive material, carcinogenic agents, gases, pesticides, fire etc., that workers are subjected to in the work premises.

Industry experts have concurred that remote video auditing/inspection/investigation is highly beneficial due to the following reasons:

*Photographed/recorded audit/ inspection/investigation evidence can be analysed/reviewed more thoroughly*

It is well-accepted that a camera can pick up minute details which an auditor/ inspector/ investigator may glance over while carrying

out a physical site audit/ inspection/ investigation. Also, still images and recorded videos give the auditor/inspector/investigator more time and flexibility to reflect on what is being displayed in front of them.

*There are several opportunities for improving the quality of the audits/ inspections/ investigations*

A remote video auditing/ inspection/ investigation allows the auditors/inspectors to capture and record vital evidence, and then easily store it for later analysis/review. Thus, if something was missed during the initial audit/inspection/investigation process, a recording of the walkthrough has been captured which can be analysed/reviewed later for accuracy. In some cases, this analysis/review can prove that the project was completed correctly the first time. While, in other cases, further review of the *video documentation* can demonstrate that the auditor/inspector did a poor job initially, and a key quality control issue was overlooked. This is generally known as video debriefing.

Remote video auditing/ inspection/ investigation services

Organizations nowadays employ third-party remote video auditing/ inspection/ investigation services to monitor security, compliance, quality, hygiene, and other issues at their premises. These services are being availed by organisations in various verticals such as healthcare, retail, banking,

manufacturing, hospitality, food delivery, and so on.

Generally, these services work with the existing cameras installed in the premises of the respective organisation. In some cases, specialised motion sensors are also installed to record relevant activity. Highly trained auditors/inspectors/investigators then connect remotely via the internet/VPN (virtual private network) to the video recording devices at the respective premises. The auditors/inspectors/investigators then scrutinize the video recordings and ascertain whether everything is in order with respect to the processes, the equipment, the staff, and several other parameters. They generate an audit/inspection/investigation report of their findings and share it with the concerned stakeholders. However, in some cases like that of banks, since the auditors/inspectors/investigators may not have sufficient situational awareness about the respective premises, it is likely that they may tend to report false positives.

It is also well-known that some of these remote video auditing/ inspection/ investigation services offer automated features like video analytics (motion /object/perimeter detection, face recognition, etc.), artificial intelligence/ machine learning etc. However, experts have expressed concerns about the efficacies of these systems since any automated system can detect only what it has been programmed for. What about the rest? Also, the permutation combinations of exceptions can be so vast and varied that it

is both highly improbable and impossible to automate every kind of exception, including the unexpected ones. Further, these automated systems tend to trigger false alarms thereby increasing the burden of the auditors/inspectors. Moreover, technologies like face recognition raise many ethical and privacy concerns.

Given the above considerations, it is not uncommon for organizations to deploy their own audit teams to oversee and supplement third-party remote video auditing/ inspection/investigation services, ensuring comprehensive monitoring and accurate analysis of video footage. COM-SUR provides a robust solution that empowers organizations to conduct effective video auditing/inspection/ investigation, whether through third-party services or in-house teams, thereby enhancing the overall integrity and reliability of the auditing process.

#### CHALLENGES FACED BY AUDITORS WHEN WORKING WITH SURVEILLANCE VIDEO

1. Auditors, whether internal or external, encounter several challenges when working with surveillance video due to the lack of specialized tools that offer ease, efficiency, and standardization in video analysis.
2. Auditors are often tasked with investigating extensive periods of surveillance video, ranging from days to months, which can be a daunting and time-consuming task. This becomes even more challenging when auditors are also responsible for audits in



other areas unrelated to surveillance video, resulting in a limited sample size for video-related audits.

3. Playback of multiple cameras simultaneously, especially over the internet, poses difficulties due to the large file size of videos. Auditors require flexibility in terms of seamless navigation, zooming, panning, frame-by-frame playback, video enhancement, bookmarking, easy documentation of findings, quick reporting, and video extraction.

4. The absence of tools enabling simultaneous playback of videos from diverse camera types and frame rates makes it challenging for auditors to connect and analyze various pieces of information, hindering their ability to present a cohesive story in a single video file.

5. The use of disparate surveillance video systems with proprietary video formats creates challenges in aggregating and playing back relevant video footage.

6. Issues such as inadequate backup facilities, malfunctioning cameras, or recording devices with data loss due to hardware failures can result in crucial data being unavailable to the auditor.

7. Certain surveillance video systems are programmed to record video only when specific events or triggers occur, such as motion detection or perimeter intrusion. This limits the auditor's ability to review extended periods of video before and after such events, as most systems retain only a few

minutes of pre- and post-trigger footage.

8. Tampering or insider interference with the surveillance system can result in the loss of data, rendering it unavailable to auditors.

9. The responsibility for investigating surveillance video often falls solely on the auditor, as there may be no established culture of in-house personnel conducting video audits at the respective site.

10. Limited proficiency of IT or technical staff with the surveillance video system can further burden the auditor, who may require assistance or expertise beyond their own capabilities.

Addressing these challenges requires a comprehensive solution that empowers auditors with specialized tools, standardized processes, and efficient workflows. COM-SUR serves as a powerful software solution designed to streamline video analysis, overcome these obstacles, and enable auditors to conduct effective and thorough investigations of surveillance video footage.

ADDRESSING THE RISK OF OVERRELIANCE ON TECHNOLOGY ARISING FROM THE USE OF AUTOMATED TOOLS AND TECHNIQUES (ATT) AND FROM INFORMATION PRODUCED BY AN ENTITY'S SYSTEMS

International Auditing and Assurance Standards Board (IAASB) has published a Frequently Asked Questions document (dated March 2021) that helps auditors address the

risk of overreliance on technology, whether it arises from using automated tools and techniques or from using information produced by an entity's systems.

Here are some relevant excerpts from the above document (see link at the end of these observations):

Page 1

"... As technology evolves and new approaches to auditing develop, the relevance of a particular ATT (automated tools and techniques) and its relative advantages may change..."

Page 2

"...The use of technology may potentially create biases or a general risk of overreliance on the information or output of the audit procedure performed (i.e., "risk of overreliance")..."

"...Overreliance may take numerous forms such as not understanding an ATT being used, or assuming the outputs of an ATT, or an entity's system, are appropriate for use without further consideration. Overreliance on technology can be the cause of, or result from, a lack of professional scepticism, or professional judgment..."

"...Using technology may also give rise to other auditor biases, for example automation bias. Automation bias is a tendency to favor output generated from automated systems, even when human reasoning or contradictory information raises questions as to whether such output is reliable or fit-for-purpose. As a result, the risk of overreliance on the

information or technology is increased..."

<https://www.ifac.org/system/files/publications/files/IAASB-Automated-Tools-Techniques-FAQ.pdf>

Disclaimer: COM-SUR and Hayagriva Software are not a part of IFAC and such use of IFAC's copyrighted material in no way represents an endorsement or promotion by IFAC of name of Hayagriva Software or its products or services. Any views or opinions that may be included in this paper are solely those of Hayagriva Software, and do not express the views and opinions of IFAC or any independent standard setting board associated with IFAC.

#### OTHER GOOD READING

The impact of Covid-19 on Audit and Assurance – challenges and considerations – Association of Chartered Certified Accountants, 2020 (ACCA)

The above report is based on practical experiences shared by members of ACCA's Global Forum for Audit and Assurance. The report highlights several issues that auditors are required to focus on during these challenging times of the pandemic.

Here is a relevant excerpt (see link at the end of these observations):

"... Auditors must ensure that they can rely on the technology they are planning to use and remain sceptical when observing the process. For example, they may need to consider asking their company staff to show them a clear view of the entire warehouse before the inventory

count starts, which will avoid restricting themselves in choosing to test items that are only visible during the videocall. It is also very important that the process followed is well documented.

Some practical examples noted by ACCA's Audit and Assurance global forum members included:

1. Participation of more than one member of the audit team during observation through video-conferencing equipment to enhance the observation capabilities and mitigate the risk.
2. Selecting more items to test during observation than usual.
3. Taking screenshots during the observation to enhance the evidence..."

[https://www.accaglobal.com/content/dam/ACCA\\_Global/img/respcam/Coronavirus/The%20Impact-of-Covid-19-on-Audit-and-Assurance-challenges-and-considerations.pdf](https://www.accaglobal.com/content/dam/ACCA_Global/img/respcam/Coronavirus/The%20Impact-of-Covid-19-on-Audit-and-Assurance-challenges-and-considerations.pdf)

ISO 9001 Auditing Practices Group Guidance on: REMOTE AUDITS (published in April 2020)

The above document published by the International Organization for Standardization (ISO) in collaboration with the International Accreditation Forum stresses on the importance of remote auditing in the wake of the COVID-19 pandemic and suggests some guidelines.

[https://committee.iso.org/files/live/sites/tc176/files/documents/ISO%209001%20Auditing%20Practices%20Group%20docs/Auditing%20General/APG-Remote\\_Audits.pdf](https://committee.iso.org/files/live/sites/tc176/files/documents/ISO%209001%20Auditing%20Practices%20Group%20docs/Auditing%20General/APG-Remote_Audits.pdf)

THE SOLUTION – COM-SUR – THE WORLD'S ONLY CCTV/SURVEILLANCE VIDEO FOOTAGE AUDITING, SMART BACKUP, AND STANDARDIZED INTELLIGENT INCIDENT REPORTING SOFTWARE – THE MISSING PIECE OF CCTV/SURVEILLANCE VIDEO

COM-SUR is a CCTV/surveillance video footage auditing, smart backup, and standardized intelligent incident reporting software that serves as a complete workflow and force multiplier. It helps audit 24 hours of footage in minutes, reduces data size, creates standardized intelligent reports, and delivers business intelligence. COM-SUR helps unlock hidden information in CCTV/surveillance video footage and enables people to gain actionable intelligence, improve homeland security, prevent crime and losses, identify and mitigate threats and hazards, and improve operational efficiency. It empowers people to gain new jobs as CCTV/surveillance video footage auditors and start new businesses of auditing video footage. Like MS Office, COM-SUR is an enabler that makes it easy to work with CCTV and other surveillance cameras in a standardized way, leading to better decision-making. It also offers exceptional investigative capabilities.

The advantages of auditing CCTV footage as a standard operating procedure by every user of CCTV have already been explained in each of the 'UTILITY VALUE OF COM-SUR' papers.

## COM-SUR 'ULTIMA' – THE IDEAL TOOL FOR AUDITORS

In order to carry out either a physical or remote audit that involves surveillance video, it is recommended that the audit team should make use of COM-SUR 'ULTIMA', the highest version of COM-SUR. Along with COM-SUR 'ULTIMA', auditors will find 'RIP-IT', a video frame extraction tool to also be an invaluable tool.

## COURSE

To understand how to use COM-SUR 'ULTIMA' and 'RIP-IT', it is recommended to take the Advanced CCTV video footage auditing and investigation course, which is available on Udemy.

## HOW COM-SUR WILL HELP AN AUDIT TEAM

### EXPLAINING THE SCENARIOS

Here are the scenarios for an auditor to investigate surveillance video using COM-SUR ('ULTIMA'), which needs to be installed on the auditor's laptop:

1. On-site: When the auditor visits the site physically and carries out the investigation of the videos on-site.
2. Remotely: When the auditor carries out the investigation of the videos without visiting the site

In both the above cases, there can be a scenario where COM-SUR has been deployed on-site, and it is a standard operating

procedure of the organization to audit the footage daily by a relevant team on site, thereby making the investigation task far easier for the overseeing auditor.

3. External video: When video evidence is received for investigation. For example, it could be an incident captured on video (from a mobile phone, drone, body-worn or CCTV camera), or video evidence regarding an issue provided by a whistle-blower that needs to be investigated.

Push Audit: Further, there can be a scenario where COM-SUR has been deployed on-site and COM-SUR's Push Audit plugin has also been opted for. In this case, screenshots captured by COM-SUR are re-converted into video, further reduced in size, and 'pushed' to the user's account with Google Drive, OneDrive, and Dropbox, every four hours. This solution is especially useful for organizations that have several sites and wish to centralize their video surveillance activities without making huge investments on resources like hardware, manpower, connectivity and associated infrastructure.

Scenario 1: On-site where COM-SUR has been deployed

In this case the auditor simply needs to connect his/her laptop (on which COM-SUR 'ULTIMA' has been installed) to the PC on which any COM-SUR version has been deployed, select the desired folder (by year, month, and date) containing the screenshots, and carry out the investigation activity as has been explained in the course.



Scenario 1A: On-site where COM-SUR has not been deployed

In this case the auditor needs to access the video feed from the recorder using his/her laptop (on which COM-SUR 'ULTIMA' has been installed) and carry out the investigation activity as has been explained in the course.

Scenario 2: Remotely where COM-SUR has been deployed

In this case, the auditor simply needs to do the following:

1. Where an organization has made arrangements to save the screenshots to a cloud service (as may be supported by COM-SUR) or to the organization's own server, the auditor simply needs to select the desired folder (by year, month, and date) containing the screenshots, and carry out the investigation activity as has been explained in the course. The auditor should access the screenshots using his/her laptop on which COM-SUR 'ULTIMA' has been installed.

2. Remotely access the PC (using any remote viewing software) on which COM-SUR has been deployed, select the desired folder (by year, month, and date) containing the screenshots, and carry out the investigation activity as has been explained in the course. The auditor should access the above PC using his/her laptop on which COM-SUR 'ULTIMA' has been installed.

Scenario 2A: Remotely where COM-SUR has not been deployed

In this case, the auditor needs to access the video feed from the recorder using his/her laptop (on which COM-SUR 'ULTIMA' has been installed) and carry out the investigation activity as has been explained in the course. Steps to be followed by the auditor to work with COM-SUR in case of Scenarios 1 and 2 In case of Scenarios 1 and 2, where COM-SUR has been deployed on-site, the auditor needs to connect his/her laptop (on which COM-SUR 'ULTIMA' has been installed) to the PC on which any COM-SUR version has been deployed. In order to understand how this works, please click the link below:

<https://www.comsur.biz/Whitepaper - Steps to be followed by an auditor to work with COM-SUR - Template no. 5.7a.pdf>

Scenario 3: External video (selective frames)

In this case, the auditor simply needs to play the video in the respective media player on his/her laptop and capture relevant frames (which he/she deems important) using the manual capturing abilities offered by COM-SUR 'ULTIMA', as has been explained in the course. The auditor can then carry out the investigation activity on these selected frames using COM-SUR 'ULTIMA', as has been explained in the course.

Scenario 3A: External video (all frames)

In this case, the auditor first needs to extract the frames of the video using 'RIP-IT', a video frame extraction tool. Then he/she can access these frames through COM-SUR 'ULTIMA' (which has been installed on his/her laptop) and carry out the investigation activity as has

been explained in the course.

Scenario: COM-SUR's Push Audit plugin

In this case, the auditor receives the links to the respective videos. He/she can then audit these videos either by downloading them from the link, or by playing the videos from the respective link itself. This facility of playing videos from links is provided by services such as Google Drive, OneDrive, and Dropbox. Here is an explanation of how the auditor can access the respective videos from each of these services:

Google Drive – The auditor will be able to play the entire video from the respective Google Drive link opened in a browser. The auditor can also download the video from the link.

OneDrive - The auditor will be able to play the entire video from the respective OneDrive link opened in a browser. The auditor can also download the video from the link.

Dropbox – The auditor will be able to play a 15-minute preview of the video from the respective Dropbox link opened in a browser. In order to access the entire video, Dropbox offers the facility of downloading the video from the link, as well as adding the link to the team's Dropbox account (this can be done by logging in to the respective Dropbox account).

To know more about COM-SUR's Push Audit plugin, please write to us at [pushaudit@comsur.biz](mailto:pushaudit@comsur.biz).

## CONCLUSION

"You see, but you do not observe" is a quote by Sherlock Holmes in A Scandal in Bohemia (1891, written by Sir Arthur Conan Doyle). COM-SUR makes 'observation' far effortless and effectual leading to superior results.

"Cameras don't lie" - but how will you know unless you 'see' what the cameras 'saw'?  
Audit video - why suffer!

Get award-winning COM-SUR now. Don't wait for things to go wrong!