
com sur™
the missing piece of CCTV
THE FOOTAGE WHISPERER
"SEE WHAT THE CAMERA SAW"
GET THE BOOK
100+ TOPICS - AIRPORTS TO ZOOS
GAUTAM D. GORADIA

# UTILITY VALUE OF COM-SUR™ FOR GOVERNANCE

## WELCOME

## AUDIT HOURS OF FOOTAGE IN MINUTES FIND OUT HOW COM-SUR, THE BEST 'MOUSETRAP' WILL HELP

"Seeing is believing - See what the camera saw"

CCTV and other forms of video surveillance are commonly used by government agencies world over, but footage is often only reviewed reactively. Our company realized this problem early-on and has developed the world's only CCTV video footage auditing software that encourages daily auditing (hours in minutes) of CCTV footage, filling the gap for a complete "workflow". The software works with existing cameras and VMS, regardless of type/brand, and provides a standardized approach for intelligent incident reporting. Our software also offers exceptional investigative capabilities.

## '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 the world's only 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.

## HOW COM-SUR SMARTLY REDUCES 'VIDEO' STORAGE SIZE

COM-SUR employs an innovative approach to

 

smartly reduce the amount of video to be audited and consequently the storage size of videos. Regardless of the video's frame rate, COM-SUR captures a single screenshot of the consolidated 'moment' of 'that' one second, when the I, P, and B frames come together. This method significantly reduces data size without sacrificing vital information. It goes without saying that when multiple cameras are displayed in a grid view, say 4x4, the storage size is further reduced since all the cameras are captured as a single image. Since no suggestion is being made to replace the actual video with screenshots, COM-SUR acts as a wonderful supportive technology both to audit (review) just 86400 frames representing 24 hours and reducing the data size at the same time.

## WHY AUDITING IS IMPORTANT FOR A NATION'S GOVERNANCE

Governance is defined as the sum of all the processes of governing, undertaken by the government of a state, by a market, or by a network over a social system (family, tribe, formal or informal organization, a territory or across territories) and through the laws, norms, power or language of an organized society. It includes activities that ensure a public sector entity's credibility, establish equitable provision of services, and assure appropriate behaviour of government officials thereby reducing the risk of public corruption.

Auditing is the foundation of good public sector governance. Auditing helps public sector organizations achieve accountability and integrity, improve operations, and instil confidence among citizens and stakeholders help by providing unbiased, objective assessments of whether public resources are managed responsibly and effectively to achieve intended outcomes. The public sector auditor's role complements the governance responsibilities of oversight, insight, and foresight. Oversight checks whether public sector entities are doing what they are supposed to do and serves to detect and deter public corruption. Insight helps decision-makers by providing an independent assessment of public sector programs, policies, operations, and results. Foresight recognizes trends and emerging challenges. In order to fulfil each of these roles, auditors employ tools such as financial audits, performance audits, investigations, and advisory services.

It is well-accepted that public trust is a vital part of an effective governance. However, several recent studies by the Organization for Economic Co-operation and Development (OECD) (https://www.oecd.org/) portray a dramatic decline in public trust in national governments worldwide. This decline could lead to serious implications for governments around the world. In this context, experts have concurred that auditing how the government is functioning, and how is it allocating its resources, and making the audit reports accessible, would greatly help to rebuild trust with the public.

## SUPREME AUDIT INSTITUTIONS – THEIR VALUE AND BENEFITS IN MAKING A DIFFERENCE TO THE LIVES OF CITIZENS

Supreme Audit Institutions (SAIs) are the topmost audit institution of a country. They are known mainly for their role in overseeing the management of public finances, i.e., government revenue and expenditure. Many SAIs also carry out an audit of public entities' compliance with rules and regulations, and the performance of government programs and policies. By scrutinizing public financial

management and performance, SAIs provide assurance that public resources are used prudently and efficiently for the benefit of the citizens.

The International Organization of Supreme Audit Institutions (INTOSAI) is an intergovernmental organization having 193 members who are Supreme Audit Institutions in their respective countries (for example, the Comptroller and Auditor General of India is the Supreme Audit Institution of India, the Government Accountability Office of the United States, and so on). INTOSAI has released a set of principles christened INTOSAI-P 12 which emphasise that the extent to which a Supreme Audit Institution (SAI) is able to make a difference to the lives of citizens depends on the SAI.

https://www.intosai.org/fileadmin/downloads/documents/open_access/INT_P_11_to_P_99/INTOSAI_P_12/INTOSAI_P_12_en_2019.pdf

These principles are summarised as follows:

Principle 1: Safeguarding the independence of SAIs.

Principle 2: Carrying out audits to ensure that government and public sector entities are held accountable for their stewardship over, and use of, public resources.

Principle 3: Enabling those charged with public sector governance to discharge their responsibilities in responding to audit findings and recommendations and taking appropriate corrective action.

Principle 4: Reporting on audit results and thereby enabling the public to hold government and public sector entities accountable.

Principle 5: Being responsive to changing environments and emerging risks.

Principle 6: Communicating effectively with stakeholders.

Principle 7: Being a credible source of independent and objective insight and guidance to support beneficial change in the public sector.

Principle 8: Ensuring appropriate transparency and accountability of SAIs.

Principle 9: Ensuring good governance of SAIs.

Principle 10: Complying with the SAI's Code of Ethics.

Principle 11: Striving for service excellence and quality.

Principle 12: Capacity building through promoting learning and knowledge sharing.

## CHALLENGES FACED BY GOVERNMENT AGENCIES

1. Terrorism:

Government agencies are often targets of terrorist attacks due to their role in enforcing laws and policies. Attacks may be aimed at specific government buildings, such as courthouses or legislative offices, or at high-profile events or individuals.

2. Unauthorized access:

Government agencies need to ensure that only authorized personnel are allowed inside their

premises, and that visitors do not have access to restricted areas.

3. Espionage:

Government agencies often deal with sensitive and classified information, making them targets for espionage activities, especially by foreign intelligence agencies.

4. Threats to critical infrastructure:

Government agencies are responsible for maintaining critical infrastructure, such as power grids, nuclear plants, water treatment plants, bridges, airports, ports which need to be protected from various threats like terror attacks, vandalism, arson, sabotage, and so on.

5. Insider threats:

Government agencies have to deal with insider threats from disgruntled employees or even unwitting staff who fail to follow proper security and safety measures.

6. Disaster management issues:

In the wake of a disaster, natural or otherwise, government agencies need to assess the same and plan and implement rescue efforts accordingly.

7. Compliance issues:

Government agencies need to comply with various regulations and guidelines.

8. Humongous growth of surveillance video:

The exponential growth of surveillance cameras has resulted in an unprecedented surge in surveillance video. Effectively managing this data has become a daunting challenge due to the massive storage capacity required, especially considering the prolonged retention periods necessary for security, incident investigation, or legal purposes. Furthermore, the prevalence of high-resolution video with increasing megapixels compounds the storage demands, making efficient data management an urgent priority for organizations grappling with the immense volume of surveillance footage.

## COVID-19 PANDEMIC

The pandemic severely impacted the functioning of government agencies worldwide. Government agencies had to enforce restrictions/lockdowns as well as implement various measures in order to curb outbreaks.

## USE OF VIDEO SURVEILLANCE BY GOVERNMENT AGENCIES

Government agencies use video surveillance to monitor a wide range of areas, depending on their specific responsibilities and priorities. Here are some examples of areas that government agencies may monitor using video surveillance:

1. Public spaces:

Government agencies may use video surveillance cameras to monitor public spaces, such as parks, streets, and other areas where people gather, in order to check for public safety issues, identify criminal activity, and respond to emergencies.

2. Transportation hubs:

Transportation hubs, such as airports, train

stations, and bus terminals, are monitored using video surveillance for security threats, identifying potential safety hazards, and ensuring the efficient flow of traffic.

3. Government facilities:

Government facilities, such as courthouses, municipal buildings, and military installations, are monitored using video surveillance, for security threats and responding to emergencies.

4. Border crossings:

Border crossings are monitored using video surveillance to help prevent illegal immigration, drug trafficking, and other security threats.

5. Critical infrastructure:

Critical infrastructure, such as power plants, nuclear plants, water treatment facilities, and communication networks, may be monitored using video surveillance to help prevent sabotage, accidents, and other security threats.

6. High-risk areas:

Government agencies use video surveillance to monitor high-risk areas, such as prisons, military zones, and areas prone to natural disasters for various threats and responding to emergencies.

7. Disaster management:

Government agencies use video surveillance for disaster management in several ways such as follows:

a. Real-time situational awareness during a disaster to assess the extent of damage and areas that require immediate attention.

b. Aiding emergency response efforts by obtaining critical information about the disaster and the movement of people and vehicles.

c. Post-disaster analysis to assess the impact of a disaster and determining rescue efforts.

d. Monitoring public safety during a disaster.

Further, in a government facility, various areas may be monitored using video surveillance, depending on the specific facility and its security needs. Here are some common areas that are monitored:

- Entry and exit points
- Public areas
- Restricted areas
- Computer/Server rooms
- Hallways and corridors
- Stairwells and elevators
- Parking areas

Besides CCTV cameras, government agencies also use other forms of video surveillance as follows:

1. Drones:

Government agencies use drones to monitor their premises from the air which is useful for identifying security threats, monitoring for suspicious behavior, and responding to emergencies. Drones are also be used to inspect hard-to-reach areas, such as rooftops

or other elevated structures.

2. Body worn cameras:

Government agencies usually equip their personnel with body worn cameras to capture video footage of their interactions with the public. Body worn cameras can be useful for documenting incidents, providing evidence in legal proceedings, and promoting transparency and accountability.

3. Dash cams:

Government agencies use dash cams in their vehicles to capture video footage of traffic stops, pursuits, and other interactions with the public. Dash cams are useful for documenting incidents and providing evidence in legal proceedings. They also help in promoting transparency and accountability.

## LIVE MONITORING – CHALLENGES

Most government agencies have a dedicated control room with operators, set up for live monitoring of CCTV cameras as well as other cameras such as drones, body worn cameras, dash cams etc. However, live monitoring comes with its own set of challenges of video blindness, poor attention span, boredom, operator bias, false alerts, and so on. Moreover, these cameras continuously capture and record humungous amounts of video data. It therefore becomes a daunting task for the operators to review and analyse this data whenever the need arises. Thus, it may be noted that benefits from video surveillance systems can accrue only when they are used optimally, suggestions for which are enumerated further on, in this document.

## COMPLIANCE - GENERAL

Conformity or compliance in any organization means adherence to laws and/or rules and regulations, various standards, as well as data storage and security requirements as laid down by government bodies, governing bodies of the respective industry, or the management of the organization. When an organization complies with the requirements mandated by government and/or governing bodies, then it is termed as 'regulatory compliance' which enables the organization to run in a legal and safe manner.

## COMPLIANCE - AUDITS

Several organizations carry out compliance audits on a regular basis to avoid the potential consequences of non-compliance.
A compliance audit examines how well an organization adheres to compliance requirements. Some organizations use video surveillance to monitor compliance issues and audit recorded video footage from time to time for investigating and preventing compliance issues. Auditing video provides actionable insights on the level of compliance within the organization.

## AUTOMATED SOFTWARE – WHY THEY WILL NOT WORK IN ISOLATION

In the wake of the Christchurch shooting incident, several high-profile places of worship considered deploying gun detection technology. However, there are concerns about its efficacy, since it may not be able to detect all types of weapons, or the perpetrator could still create damage before being detected. Similarly, automated systems like video analytics, AI/ML can only detect what they have

been programmed for. What about the rest? Again, these technologies are prone to triggering huge amounts of false alarms. Also, since the permutation combinations of exceptions can be vast and varied, it becomes almost impossible to automate every kind of exception. Facial recognition technology also raises ethical and privacy concerns, and has been found to produce inaccurate results, especially for certain ethnic groups. Therefore, experts suggest that while automated technologies will continue to grow, human intervention and intelligence will still be necessary to verify alerts and ensure their efficacy.

## "CCTV AND OTHER FORMS OF VIDEO SURVEILLANCE ARE NOT ENOUGH – WE MAKE IT WORK FOR YOU"

While it is not being suggested that optimal usage of video surveillance can cure all issues, several issues of the following kind can be addressed by doing just a little 'more' with respect to making the optimal use of video surveillance systems:

- Recces/suspicious movements/activities

- Insider job/security lapses

- Bullying/violence/disputes

- False allegations and/or claims

- Sexual harassment and/or other kinds of abuse

- Unauthorized/unlawful activities

- Fraud/loss/theft

- Employee performance issues

- Compliance issues

- Disaster management issues

- Intrusions, especially by animals

- Inattentive staff (e.g. guard sleeping)

- Housekeeping issues

- Cameras/recorder malfunctions

So, what is the 'more' that needs to be done?

## 1) AUDIT CCTV AND OTHER SURVEILLANCE VIDEO FOOTAGE DAILY AS A STANDARD OPERATING PROCEDURE

'Auditing' means 'seeing' what the cameras 'saw'. Auditing of CCTV and other surveillance video footage should be done daily (continuous investigation) to identify potential issues and threats. Auditing is a dedicated and systematic process that helps address challenges related to live monitoring and alert-based systems. Auditing helps in evaluating analyzing incidents to improve existing policies, procedures, and processes. Concerned personnel should be trained to become video footage auditors, and the audit teams should be rotated to avoid complacency/collusion. Daily auditing of CCTV and other surveillance video footage can also help in adhering to the principles of Kaizen and TQM for business improvement.

## 2) DOCUMENT AUDIT FINDINGS/INCIDENTS

Audit findings/incidents should be documented in a standardized template to find the root cause to prevent future recurrences. Historical

data of such findings/incidents can reveal patterns that can help take better informed corrective and preventive action. If all government agencies report incidents in a standardized template, relevant authorities can derive business intelligence from the data and take action for the collective benefit of all concerned stakeholders.

3) ENSURE DISASTER RECOVERY OF CCTV AND OTHER SURVEILLANCE VIDEO FOOTAGE – LIKE A 'BLACKBOX'

CCTV and other surveillance video footage must be stored at multiple locations in order to ensure that even if the recorder/storage device is stolen, destroyed or tampered with the data is never lost. Further, any backed-up data must easily be searchable and retrievable; else, it is going to be a nightmare finding the relevant video.

4) DISPLAY DYNAMIC INFORMATION AT RELEVANT PLACES

Document and display details of information that is dynamic in nature in relevant areas. For example:

1. List of authorised personnel working in the government agency's premises.

2. List of authorized security personnel deployed at the government agency's premises.

3. List of habitual offenders/suspects likely to visit the government agency's premises (a 'Watch out' list).

5) USE A POWERFUL NEW SIGNAGE

"WE AUDIT CCTV VIDEO FOOTAGE EVERYDAY".

One size, one color, one powerful message. Across the nation.

DE-CENTRALIZED SURVEILLANCE + CENTRALIZED SURVEILLANCE = OPTIMAL RESULTS

Organizations with multiple locations struggle with centralized video surveillance due to infrastructure cost, internet bandwidth, and operator limitations. De-centralized surveillance offers higher accountability at each location and better situational awareness, leading to more chances of discovering exceptions.

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!

**Finally, allow us to present three important mantras that change the landscape of video surveillance:**

**1. Auditing is fundamental – everything else is peripheral.**

 

2. Cameras have lenses – humans have eyes.

3. Let's make cameras 'accountable'.