

comTM
sur

the missing piece of CCTV

GET THE BOOK
INTERNATIONAL PRICING



**"SEE WHAT THE
CAMERA SAW"**

IN 95% LESS TIME

**KNOW WHAT YOU DON'T KNOW
TURN GARBAGE TO GOLD**

**THE DEFINITIVE GUIDE TO
VISUAL EVIDENCE GOVERNANCE**



**BUILD 'BETTER' AI
POWERED BY DAILY AUDITS**

100+ SECTORS - AIRPORTS TO ZOOS

GAUTAM D. GORADIA



VISUAL EVIDENCE
GOVERNANCE IN THE
REALM OF VIDEO
SURVEILLANCE



VISUAL EVIDENCE GOVERNANCE (VEG)

Across the world, there are well-established discussions around Information Governance, Data Governance, AI Governance, Corporate Governance, Security Governance, and Risk Governance. Each of these exists because organizations realized that merely possessing information, technology, systems, or infrastructure is not enough. They must be governed.

However, in the realm of video surveillance, one critical question has largely been ignored:

Who is governing the visual evidence?

CCTV cameras are increasing everywhere. From airports to zoos (A to Z). Alongside this, there is

growing excitement around AI, video analytics, facial recognition, object detection, behaviour detection, command centres, dashboards, and real-time alerts. All of this may be useful. But it still does not answer the core question.

Are we governing the visual evidence generated by these cameras?

Visual Evidence Governance, or VEG, refers to the structured discipline of reviewing, auditing, documenting, preserving, escalating, and acting upon visual evidence generated by CCTV and other video systems in a systematic, demonstrable, and accountable manner.

The issue is not whether cameras exist. The issue is whether the footage generated by those cameras is being reviewed, understood, documented, preserved, and acted upon.

For decades, the surveillance industry has focused on installation, recording, storage, transmission, live monitoring, and now AI-based detection. These are important, but they are not governance. Governance begins only when visual evidence enters a structured workflow.

Was the footage reviewed? Who reviewed it? What was found? What was escalated? What was preserved? What action was taken? What pattern emerged over time? What feedback was generated for management, compliance, operations, investigation, or AI improvement?

Without this discipline, CCTV footage becomes *Dark Data*. It exists, but it is not meaningfully used. It sits inside DVRs, NVRs, VMS platforms, servers, hard disks, or cloud storage until it is overwritten, lost, stolen, corrupted, ignored, or viewed only after an incident.

Ishikawa Framework for Visual Evidence Governance

The Ishikawa Framework for Visual Evidence Governance (please see page no. 7) explains how massive volumes of CCTV footage remain *Dark Data* when there is no structured auditing, reporting, governance, preservation, or human review.

Through disciplined auditing workflows, standardized reporting, and continuous human feedback, Visual Evidence Governance converts passive footage into Governed Visual Intelligence. This distinction is important because live monitoring is not the same as auditing. Live monitoring depends on real-time human attention, but human beings cannot continuously watch dozens, hundreds, or thousands of video feeds effectively for long periods. Operator fatigue, distraction, video blindness, and divided attention are real limitations.

Similarly, AI is not a complete answer. AI can help

detect what it has been trained or programmed to detect. It can flag, classify, alert, and assist. But it cannot automatically understand every context, every intent, every evolving risk, every insider pattern, every operational deviation, every false positive, or every false negative.

Eventually, someone must review, interpret, validate, escalate, and decide. That someone is human.

Therefore, the real challenge is not to remove the human from surveillance. The real challenge is to make human review faster, easier, structured, standardized, accountable, and useful.

This is where the structured Daily CCTV Video Footage Auditing Chart becomes important (please see page no. 8).

When CCTV audit findings are recorded in a structured chart, every human observation and every AI-flagged event can become a structured data point. Over time, this can support dashboards, timelines, heatmaps, trend analysis, compliance records, incident reports, and management intelligence. It also helps build Better AI.

AI in video surveillance needs real-world, site-specific, human-validated feedback. It needs to learn from actual environments, actual footage, actual exceptions, actual false positives, actual false negatives, and actual human interpretation. Visual Evidence Governance provides the discipline through which such feedback can be created. The future of video surveillance cannot be only about more cameras, larger storage,

smarter AI, or bigger command centres. It must also be about governance.

Visual Evidence Governance changes the central question from:

“Do we have CCTV cameras?”

to:

“Are we responsibly governing the visual evidence those cameras generate?”

That is the real shift. Because if footage is not reviewed, documented, preserved, escalated, and acted upon, then even the best cameras and the most advanced AI may still fail to deliver prevention, accountability, compliance, intelligence, or trust.

As cameras continue to multiply globally, Visual Evidence Governance may become one of the most important missing disciplines in video surveillance.

Not because it adds another camera. But because it finally asks:

What did we do with what the camera saw?

Like Information Governance, Data Governance, AI Governance, and Risk Governance, Visual Evidence Governance is built around recognizable governance principles. The difference is that these principles are applied specifically to CCTV footage and other forms of visual evidence.

Governance Principle	Application in Visual Evidence Governance
Accountability	Clear responsibility for review, reporting, preservation, escalation, and action.
Compliance	Demonstrable adherence to legal, regulatory, operational, and internal requirements.
Integrity	Maintaining the reliability, authenticity, and usability of visual evidence.
Risk Management	Reducing risks from ignored footage, missed incidents, tampering, overwriting, or misuse.
Lifecycle Management	Governing footage from capture and review to reporting, preservation, retention, and disposal.
Security	Controlled access, secure handling, and responsible use of visual evidence.

Areas of Governance

Governance as a discipline of oversight, accountability, compliance, controls, reporting, and decision-making, it exists in almost every major function:

Area	Common Governance Term
Corporate Management	Corporate Governance
Information Technology	IT Governance
Cybersecurity	Cybersecurity Governance
Data	Data Governance
Artificial Intelligence	AI Governance
Privacy	Privacy Governance
Risk	Risk Governance
Finance	Financial Governance
Audit	Audit Governance / Internal Controls
Compliance	Compliance Governance
Healthcare	Clinical Governance
Environment	Environmental Governance
ESG	ESG Governance
Safety	Safety Governance
Quality	Quality Governance

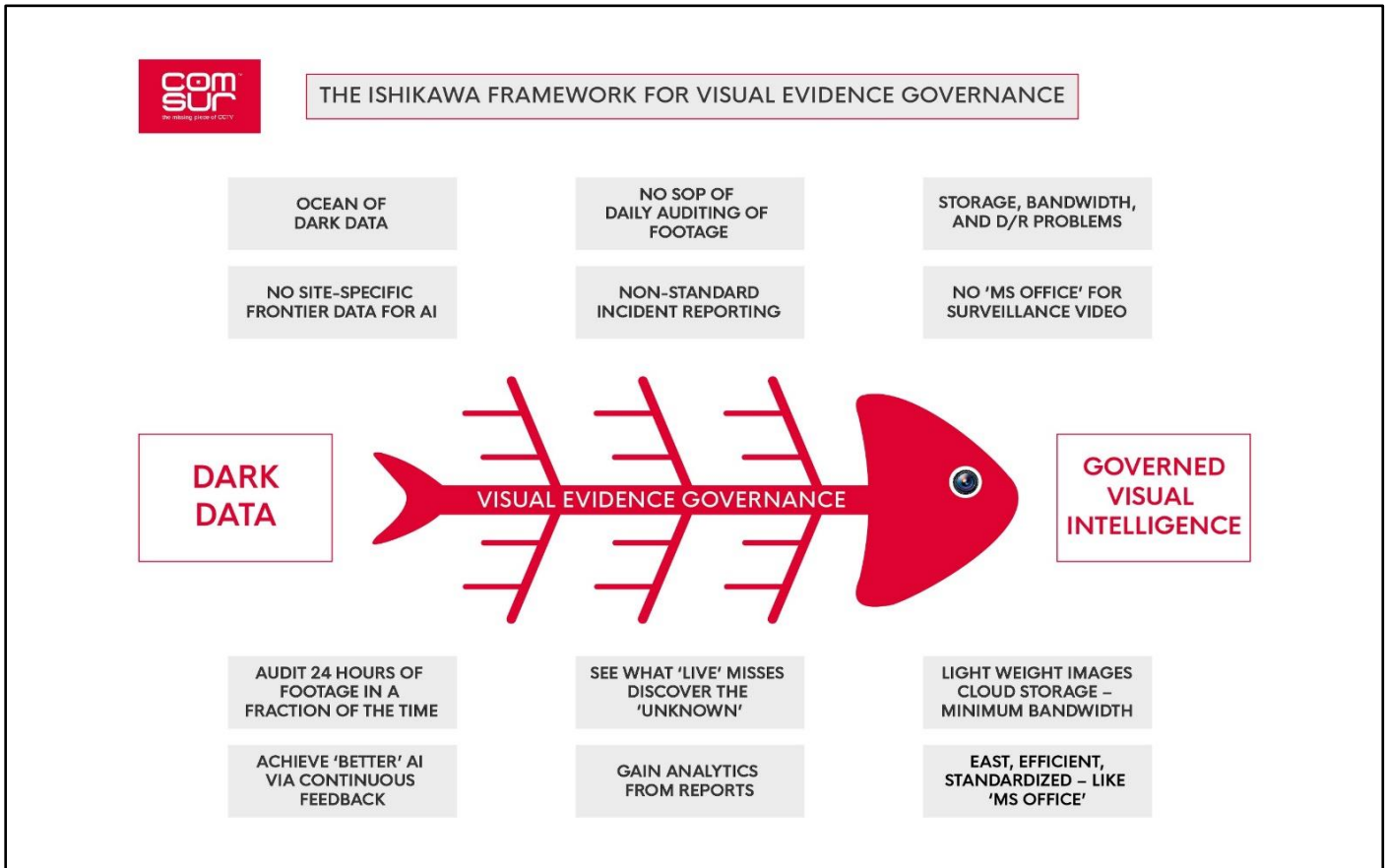
Area	Common Governance Term
Supply Chain	Supply Chain Governance
Projects	Project Governance
Procurement	Procurement Governance
Human Resources	Workforce Governance
Records & Documents	Information Governance
Public Sector	Public Governance
Intelligence & Security	Security Governance
Disaster Management	Emergency Governance
Education	Educational Governance

The common thread is:

1. Something important exists.
2. Policies and standards are defined.
3. Activities are monitored.
4. Deviations are identified.
5. Corrective actions are taken.
6. Accountability is established.
- 7 Records are preserved.

This is exactly why the term Visual Evidence Governance (VEG) is powerful.

THE ISHIKAWA FRAMEWORK FOR VISUAL EVIDENCE GOVERNANCE



DAILY CCTV VIDEO FOOTAGE AUDITING CHART

DAILY CCTV VIDEO FOOTAGE AUDITING CHART

Index:

- [Dashboard](#)
- [Auditors' Leaderboard](#)
- [Timeline](#)
- [Masters](#)

Name of Organization:

ALL DATA IS FOR ILLUSTRATION ONLY.
CLEAR LOG BOOK + PRESS CTRL + ALT + F5 BEFORE USE.

Location/Address:

IMPORTANT: To log a new entry, go to the **first available row at the end of the table** and enter the required details. Once the entry is complete, press **Ctrl + Alt + F5** to ensure that the new record is properly logged.

DATE (DD-MMM-YYYY)	CAMERA NO. & DESCRIPTION	TIME SLOT	AUDITOR	INCIDENT	REPEAT ISSUE?	HUMAN/AI	SEVERITY	STATUS	REMARKS/ACTION
12-Mar-2026	31-35 PARKING AREA	12 AM to 6 AM	DRISHTI	DRUNK / INTOXICATED PERSON	YES	HI	3	OPEN	Repeated intoxicatic
12-Mar-2026	19-20 ELEVATOR	12 AM to 6 AM	DRISHTI	VANDALISM	NO	HI	4	OPEN	Vandalism in elevatc
13-Mar-2026	21-25 CANTEEN/PANTRY	6 PM to 12 AM	DANNY	SLIP / TRIP HAZARD	NO	HI	3	WIP	Slip hazard in pantry
14-Mar-2026	5-8 CORRIDOR	12 PM to 6 PM	DRISHTI	SLIP / TRIP HAZARD	NO	HI	3	OPEN	Slip hazard in corridc

DOCUMENT FINDINGS IN ONE TAB

Total Incidents Logged

90

"OPEN" Incidents %

24%

Average Severity

2.8

Top Auditor

DRISHTI

FLAGGED BY?

HI AI

REPEAT ISSUE?

YES NO

STATUS

CLO... OPEN WIP

Incident Mix (%)

OVERCROWDING	10.0%
INAPPROPRIATE BEHAVIOUR	7.8%
ELECTRICAL HAZARD	7.8%
UNAUTHORISED ACCESS	6.7%
GUARD / STAFF ABSENT...	5.6%
DRUNK / INTOXICATED...	5.6%
LOITERING	5.6%
SLIP / TRIP HAZARD	5.6%
UNCLEAN AREA	4.4%
VANDALISM	4.4%
FIRE / SMOKE DETECTED	3.3%
COMPLIANCE VIOLATION	3.3%
CAMERA FAULT / NO VIDEO	2.2%
SUSPICIOUS PERSON	2.2%
GUARD / STAFF WASTING...	2.2%
ANIMAL INTRUSION	2.2%
SUSPICIOUS VEHICLE	2.2%
TRESPASSING	2.2%
SPITTING	2.2%
LITTERING	2.2%
HARASSMENT	2.2%
RASH DRIVING	2.2%
UNATTENDED /...	1.1%
ACCIDENT / INJURY	1.1%
SMOKING	1.1%
SECURITY BREACH	1.1%
VERBAL ALTERCATION	1.1%
VOLATILE BEHAVIOUR	1.1%
GUARD / STAFF SLEEPING	1.1%

Select Number Of Logged Days

Incident Activity (Last 15 Logged Days); Total = 19

LOCATION/TIMESLOT	6 AM to 12 PM	12 PM to 6 PM	6 PM to 12 AM	12 AM to 6 AM
1-2 MAIN GATE/ENTRANCE	0	2	4	3
21-25 CANTEEN/PANTRY	2	1	2	2
26-30 STORAGE AREA	2	4	2	7
31-35 PARKING AREA	2	5	2	4
3-4 LOBBY/RECEPTION AREA	2	7	3	2
5-8 CORRIDOR	1	4	0	0
9-18 WORK/OFFICE AREA	5	4	2	4
19-20 ELEVATOR	4	4	3	1

GAIN BUSINESS INTELLIGENCE AUTOMATICALLY